National Library of Canada
Acquisitions and Bibliographic Services Branch
395 Wellington Street
Ottawa, Ontario
K1A 0N4

Bibliothèque nationale du Canada
Direction des acquisitions et des services bibliographiques
395, rue Wellington
Ottawa (Ontario)
K1A 0N4

Your file Votre référence

Our file Notre référence

NOTICE

The quality of this microform is heavily dependent upon the quality of the original thesis submitted for microfilming. Every effort has been made to ensure the highest quality of reproduction possible.

If pages are missing, contact the university which granted the degree.

Some pages may have indistinct print especially if the original pages were typed with a poor typewriter ribbon or if the university sent us an inferior photocopy.

Reproduction in full or in part of this microform is governed by the Canadian Copyright Act, R.S.C. 1970, c. C-30, and subsequent amendments.

AVIS

La qualité de cette microforme dépend grandement de la qualité de la thèse soumise au microfilmage. Nous avons tout fait pour assurer une qualité supérieure de reproduction.

S'il manque des pages, veuillez communiquer avec l'université qui a conféré le grade.

La qualité d'impression de certaines pages peut laisser à désirer, surtout si les pages originales ont été dactylographiées à l'aide d'un ruban usé ou si l'université nous a fait parvenir une photocopie de qualité inférieure.

La reproduction, même partielle, de cette microforme est soumise à la Loi canadienne sur le droit d'auteur, SRC 1970, c. C-30, et ses amendements subséquents.

Canada

UNIVERSITY OF ALBERTA

JORDAN-CHEVALLEY DECOMPOSITIONS AND THE WEDDERBURN-MALCEV THEOREM

BY

Fernando Szechtman ©

A thesis submitted to the Faculty of Graduate Studies and Resarch in partial fulfillment of the requirements for the degree of MASTER OF SCIENCE.

DEPARTMENT OF MATHEMATICS

Edmonton, Alberta
Fall 1994

National Library
of Canada

Acquisitions and
Bibliographic Services Branch

395 Wellington Street
Ottawa, Ontario
K1A 0N4

Bibliothèque nationale
du Canada

Direction des acquisitions et
des services bibliographiques

395, rue Wellington
Ottawa (Ontario)
K1A 0N4

Your file - Votre référence

Our file - Notre référence

The author has granted an irrevocable non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of his/her thesis by any means and in any form or format, making this thesis available to interested persons.

L'auteur a accordé une licence irrévocable et non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de sa thèse de quelque manière et sous quelque forme que ce soit pour mettre des exemplaires de cette thèse à la disposition des personnes intéressées.

The author retains ownership of the copyright in his/her thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without his/her permission.

L'auteur conserve la propriété du droit d'auteur qui protège sa thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

ISBN 0-315-95117-6

Canada

Name FERNANDO SZECHTMAN

Dissertation Abstracts International is arranged by broad, general subject categories. Please select the one subject which most nearly describes the content of your dissertation. Enter the corresponding four-digit code in the spaces provided.

MATHEMATICS
SUBJECT TERM

0405
SUBJECT CODE

U·M·I

Subject Categories

THE HUMANITIES AND SOCIAL SCIENCES

COMMUNICATIONS AND THE ARTS
Architecture 0729
Art History 0377
Cinema 0900
Dance 0378
Fine Arts 0357
Information Science 0723
Journalism 0391
Library Science 0399
Mass Communications 0708
Music 0413
Speech Communication 0459
Theater 0465

EDUCATION
General 0515
Administration 0514
Adult and Continuing 0516
Agricultural 0517
Art 0273
Bilingual and Multicultural 0282
Business 0688
Community College 0275
Curriculum and Instruction 0727
Early Childhood 0518
Elementary 0524
Finance 0277
Guidance and Counseling 0519
Health 0680
Higher 0745
History of 0520
Home Economics 0278
Industrial 0521
Language and Literature 0279
Mathematics 0280
Music 0522
Philosophy of 0998
Physical 0523

Psychology 0525
Reading 0535
Religious 0527
Sciences 0714
Secondary 0533
Social Sciences 0534
Sociology of 0340
Special 0529
Teacher Training 0530
Technology 0710
Tests and Measurements 0288
Vocational 0747

LANGUAGE, LITERATURE AND LINGUISTICS
Language
- General 0679
- Ancient 0289
- Linguistics 0290
- Modern 0291

Literature
- General 0401
- Classical 0294
- Comparative 0295
- Medieval 0297
- Modern 0298
- African 0316
- American 0591
- Asian 0305
- Canadian (English) 0352
- Canadian (French) 0355
- English 0593
- Germanic 0311
- Latin American 0312
- Middle Eastern 0315
- Romance 0313
- Slavic and East European 0314

PHILOSOPHY, RELIGION AND THEOLOGY
Philosophy 0422
Religion
- General 0318
- Biblical Studies 0321
- Clergy 0319
- History of 0320
- Philosophy of 0322

Theology 0469

SOCIAL SCIENCES
American Studies 0323
Anthropology
- Archaeology 0324
- Cultural 0326
- Physical 0327

Business Administration
- General 0310
- Accounting 0272
- Banking 0770
- Management 0454
- Marketing 0338

Canadian Studies 0385
Economics
- General 0501
- Agricultural 0503
- Commerce-Business 0505
- Finance 0508
- History 0509
- Labor 0510
- Theory 0511

Folklore 0358
Geography 0366
Gerontology 0351
History
- General 0578
- Ancient 0579
- Medieval 0581
- Modern 0582
- Black 0328
- African 0331
- Asia, Australia and Oceania 0332
- Canadian 0334
- European 0335
- Latin American 0336
- Middle Eastern 0333
- United States 0337

History of Science 0585
Law 0398
Political Science
- General 0615
- International Law and Relations 0616
- Public Administration 0617

Recreation 0814
Social Work 0452
Sociology
- General 0626
- Criminology and Penology 0627
- Demography 0938
- Ethnic and Racial Studies 0631
- Individual and Family Studies 0628
- Industrial and Labor Relations 0629
- Public and Social Welfare 0630
- Social Structure and Development 0700
- Theory and Methods 0344

Transportation 0709
Urban and Regional Planning 0999
Women's Studies 0453

THE SCIENCES AND ENGINEERING

BIOLOGICAL SCIENCES
Agriculture
- General 0473
- Agronomy 0285
- Animal Culture and Nutrition 0475
- Animal Pathology 0476
- Food Science and Technology 0359
- Forestry and Wildlife 0478
- Plant Culture 0479
- Plant Pathology 0480
- Plant Physiology 0817
- Range Management 0777
- Wood Technology 0746

Biology
- General 0306
- Anatomy 0287
- Biostatistics 0308
- Botany 0309
- Cell 0379
- Ecology 0329
- Entomology 0353
- Genetics 0369
- Limnology 0793
- Microbiology 0410
- Molecular 0307
- Neuroscience 0317
- Oceanography 0416
- Physiology 0433
- Radiation 0821
- Veterinary Science 0778
- Zoology 0472

Biophysics
- General 0786
- Medical 0760

EARTH SCIENCES
Biogeochemistry 0425
Geochemistry 0996
Geodesy 0370
Geology 0372
Geophysics 0373
Hydrology 0388
Mineralogy 0411
Paleobotany 0345
Paleoecology 0426
Paleontology 0418
Paleozoology 0985
Palynology 0427
Physical Geography 0368
Physical Oceanography 0415

HEALTH AND ENVIRONMENTAL SCIENCES
Environmental Sciences 0768
Health Sciences
- General 0566
- Audiology 0300
- Chemotherapy 0992
- Dentistry 0567
- Education 0350
- Hospital Management 0769
- Human Development 0758
- Immunology 0982
- Medicine and Surgery 0564
- Mental Health 0347
- Nursing 0569
- Nutrition 0570
- Obstetrics and Gynecology 0380
- Occupational Health and Therapy 0354
- Ophthalmology 0381
- Pathology 0571
- Pharmacology 0419
- Pharmacy 0572
- Physical Therapy 0382
- Public Health 0573
- Radiology 0574
- Recreation 0575
- Speech Pathology 0460
- Toxicology 0383

Home Economics 0386

PHYSICAL SCIENCES
Pure Sciences
Chemistry
- General 0485
- Agricultural 0749
- Analytical 0486
- Biochemistry 0487
- Inorganic 0488
- Nuclear 0738
- Organic 0490
- Pharmaceutical 0491
- Physical 0494
- Polymer 0495
- Radiation 0754

Mathematics 0405
Physics
- General 0605
- Acoustics 0986
- Astronomy and Astrophysics 0606
- Atmospheric Science 0608
- Atomic 0748
- Electronics and Electricity 0607
- Elementary Particles and High Energy 0798
- Fluid and Plasma 0759
- Molecular 0609
- Nuclear 0610
- Optics 0752
- Radiation 0756
- Solid State 0611

Statistics 0463

Applied Sciences
Applied Mechanics 0346
Computer Science 0984
Engineering
- General 0537
- Aerospace 0538
- Agricultural 0539
- Automotive 0540
- Biomedical 0541
- Chemical 0542
- Civil 0543
- Electronics and Electrical 0544
- Heat and Thermodynamics 0348
- Hydraulic 0545
- Industrial 0546
- Marine 0547
- Materials Science 0794
- Mechanical 0548
- Metallurgy 0743
- Mining 0551
- Nuclear 0552
- Packaging 0549
- Petroleum 0765
- Sanitary and Municipal 0554
- System Science 0790

Geotechnology 0428
Operations Research 0796
Plastics Technology 0795
Textile Technology 0994

PSYCHOLOGY
General 0621
Behavioral 0384
Clinical 0622
Developmental 0620
Experimental 0623
Industrial 0624
Personality 0625
Physiological 0989
Psychobiology 0349
Psychometrics 0632
Social 0451

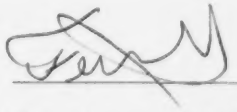
UNIVERSITY OF ALBERTA

RELEASE FORM

NAME OF THE AUTHOR	: **Fernando Szechtman**
TITLE OF THE THESIS	: **Jordan-Chevalley Decompositions and the Wedderburn-Malcev Theorem**
DEGREE	: **Master of Science**
YEAR THIS DEGREE GRANTED	: **Fall 1994**

Permission is hereby granted to the University of Alberta Library to reproduce single copies of this thesis and to lend or sell such copies for private, scholary or scientific research purposes only.

The author reserves all other publication and other rights in association with the copyright in the thesis, and except as hereinbefore provided neither the thesis nor any substantial portion thereof may be printed or otherwise reproduced in any material from whatever without the author's prior written permission.



Department of Mathematics,
University of Alberta,
Edmonton, Alberta

Date : August 30, 1994

UNIVERSITY OF ALBERTA

THE FACULTY OF GRADUATE STUDIES AND RESEARCH

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies and Research, for acceptance, a thesis entitled **JORDAN-CHEVALLEY DECOMPOSITIONS AND THE WEDDERBURN-MALCEV THEOREM** submitted by Fernando Szechtman in partial fulfilment of the degree of Master of Science.

A. Pianzola (Supervisor)

B.N. Allison (Chair)

S. Cabay, Computing Science

Date: August 25

ABSTRACT

The existence and uniqueness of the Jordan-Chevalley decomposition of an endomorphism x acting on a finite dimensional linear space $\mathbb{V}$ over a perfect field $\mathbb{K}$ into the sum of a semisimple endomorphism s and a (locally) nilpotent endomorphism n which commute are well-known facts. If $\mathbb{K}$ is not perfect or $\mathbb{V}$ is not finite dimensional neither uniqueness nor existence need to hold. We study Jordan-Chevalley decompositions with no restrictions on $\mathbb{V}$ or $\mathbb{K}$ and find necessary and sufficient conditions for the existence and uniqueness of two types of decompositions of x: separable, that is, when the semisimple part s remains semsimple after extending scalars, and standard, which means that every finite dimensional x-invariant subspace $\mathbb{U}$ of $\mathbb{V}$ is also invariant under s and n and $s|_{\mathbb{U}}$, $n|_{\mathbb{U}} \in \mathbb{K}[x|_{\mathbb{U}}]$. We then explore the intimate connection between Jordan-Chevalley decompositions and the classical version the Wedderburn-Malcev Theorem. We show that the splitting of the radical $J(A)$ of an associative and unital finite dimensional *commutative* algebra over $\mathbb{K}$ with separable quotient $A/J(A)$ is equivalent to the problem of finding the Jordan-Chevalley decomposition of an endomorphism with separable minimal polynomial.

TABLE OF CONTENTS

INTRODUCTION 1

0. PRELIMINARIES 5

0.1: Exactness 6

0.2: Semisimplicity 8

1. JORDAN-CHEVALLEY DECOMPOSITION 13

1.1: Modules over a principal ideal domain 13

1.2: Various types of endomorphisms 15

1.3: Extension of scalars 17

1.4: Eigenvalues and characteristic roots 18

1.5: Semisimplicity and extension of scalars 20

1.6: Jordan-Chevalley decomposition 22

1.7: Triangularizable endomorphisms 32

1.8: Applications. Classically separable algebras 35

1.9: Examples 38

2. SEPARABLE ALGEBRAS 43

2.1: Preliminaries 43

2.2: $(A-B)/R$ bimodules and left $A \bigotimes_R B^o$-modules 43

2.3: Separable algebras 45

2.4: Basic properties of separable algebras 49

2.5: Separable algebras over fields 56

2.6: Separable versus classically separable algebras 57

2.7: Examples 60

3. EXTENSIONS OF ALGEBRAS 63

3.1: Hochschild cohomology modules of an algebra 63

3.2: Extensions of algebras 68

3.3: Singular extensions and 2-cohomology classes of an algebra 69

3.4: Examples 77

BIBLIOGRAPHY 83

Introduction

This thesis is devoted to the study of two classical theorems and their close relationship: Chevalley Theorem on the Jordan-Chevalley decomposition of an endomorphism x of a linear space $\mathbf{V}$ over a field $\mathbb{K}$, that is, the decomposition of x as the sum of a semisimple and nilpotent commuting endomorphisms, and the Wedderburn-Malcev Theorem on the splitting of the radical $J(A)$ of an associative and unital algebra A as a direct direct summand of a subalgebra of A.

When $\mathbf{V}$ is finite dimensional and the minimal polynomial p_x of x splits over $\mathbb{K}$ one has only to triangularize each generalised eigenspace of x to obtain a decomposition of x as the sum of a diagonalizable and a nilpotent commuting endomorphisms. The same decomposition is obtained by means of the Jordan canonical form of x, a refinement of the above. If p_x does not split over $\mathbb{K}$ one may try to obtain a decomposition of x by extending scalars to the splitting field $\mathbb{L}$ of p_x over $\mathbb{K}$ hoping that the decomposition of $x_{\mathbb{L}} = 1_{\mathbb{L}} \otimes x \in End_{\mathbb{L}}(\mathbb{L} \bigotimes_{\mathbb{K}} \mathbf{V})$ is actually an extension of a decomposition of x. Although this is not true in general, Chevalley [51] showed that this is the case when $\mathbb{K}$ is perfect.

The inseparability of the eigenvalues of x over $\mathbb{K}$ lead to the consideration of a stronger type of decomposition. An absolute Jordan-Chevalley decomposition of x is a decomposition (s, n) in which the semisimple part s is absolutely semisimple, in the sense that $s_{\mathbb{F}}$ is semisimple for every extension field $\mathbb{F}$ of $\mathbb{K}$. Necessary and sufficient conditions for the existence of an absolute Jordan-Chevalley decomposition of an endomorphism acting on a finite dimensional space can be found in Bourbaki [90]. It is shown there, also in the finite dimensional case, that if absolute Jordan-Chevalley decompositions exist they are unique.

The existence and uniqueness of absolute Jordan-Chevalley decompositions in the infinite dimensional case can be found in Moody-Pianzola [to appear]. But the general problem of finding necessary and sufficient conditions for the existence and uniqueness of plain Jordan-Chevalley decompositions has not yet been solved.

In our attempt to do so we first give necessary and sufficient conditions for the existence of absolute Jordan-Chevalley decompositions with no restrictions on the the dimension of $\mathbb{V}$. The absolute Jordan-Chevalley decomposition (s, n) of an endomorphism x is standard, in the sense that every finite dimensional x-invariant subspace $\mathbb{U}$ of $\mathbb{V}$ is also invariant under s and n and the restrictions of s and n to $\mathbb{U}$ are polynomials in $x|_{\mathbb{U}}$ with coefficients in $\mathbb{K}$. It is important to note that the class of endomorphisms having a standard Jordan-Chevalley decomposition is strictly larger than the analogous class corresponding to absolute Jordan-Chevalley decompositions. Standard Jordan-Chevalley decompositions are shown to be unique and necessary and sufficient conditions for their existence are given.

Plain Jordan-Chevalley decompositions do not enjoy the nice properties possessed by the other two types of decompositions. For instance, an endomorphism x may have none or several plain Jordan-Chevalley decompositions (s, n) and an x-invariant subspace may fail to be invariant under s and n.

The general problem of existence and uniqueness of plain Jordan-Chevalley decompositions is shown to admit the following simplification:

Let p be a non-separable irreducible polynomial over $\mathbb{K}$ and x an endomorphism of a $\mathbb{K}$-linear space $\mathbb{V}$. Let $\mathbb{K}[t]$ (the $\mathbb{K}$-algebra of polynomials in the indeterminate t with coefficients in $\mathbb{K}$) act on $\mathbb{V}$ by "evaluation at x" and let $\mathbb{V}^p(x)$ be the p-primary component of the $\mathbb{K}[t]$-module $\mathbb{V}(x)$. Problem: Find necessary and sufficient conditions for the existence and uniqueness of a Jordan-Chevalley decomposition of $x|_{\mathbb{V}^p(x)}$. We give an answer to this question when x is cyclic.

Wedderburn proved his so-called Principal Theorem on the splitting of the radical of a finite dimensional associative algebra over a field of characteristic zero early this century. A generalization of this result for those finite dimensional associative algebras A over an arbitrary field $\mathbb{K}$ which are separable modulo the radical $J(A)$, i.e. $\mathbb{F} \bigotimes_{\mathbb{K}} A/J(A)$ has zero radical for every extension field $\mathbb{F}$ of $\mathbb{K}$, was later shown by Albert in 1939. The uniqueness up to conjugation of the algebra complementing the radical was proved by Malcev in 1942.

The concept of a separable algebra over a field was generalized in Auslander-Goldman [60] to algebras over an arbitrary commutative ring. This has lead to the problem of extending the Wedderburn-Malcev Theorem to algebras over commutative rings. A pioneering work in this area is Ingraham [66]. We content ourselves to give a rather general version of the Wedderburn-Malcev Theorem which suffices for our purposes of studying its relationship to Jordan-Chevalley decompositions.

In Chapter 0 of this thesis we make a review of the material that is assumed to be known by the reader. No proofs are given.

Chapter 1 deals with endomorphisms of infinite dimensional linear spaces in general and with the problem of Jordan-Chevalley decompositions in particular. The first section gives basic properties of modules over a principal ideal domain. This is a general set up for many concepts originating in Linear Algebra and Abelian Group Theory. In the second section we introduce the types of endomorphisms that we are going to deal with: semisimple, locally nilpotent, triangularizable, split, locally finite, algebraic, cyclic and diagonalizable. The third section gives a short account of a powerful tool that will be used repeatedly: extension of scalars. The fourth section discusses the relation between two concepts which agree on the finite dimensional setting: eigenvalues and characteristic roots of an arbitrary endomorphism. It was shown in Caserta [91] that they coincide when x is locally finite. We prove that this restriction is a unnecessary. Eigenvalues and characteristic roots are found in section 5 to be essential to distinguish between semisimple and absolutely semisimple endomorphisms. The sixth section covers the Jordan-Chevalley decompositions. The seventh one deals with triangularizable endomorphisms. We show how to triangularize a finite family of commuting locally finite triangularizable endomorphisms. This extends the well-known result valid in the finite dimensional case. The eighth section proves restricted versions of the Wedderburn-Malcev Theorem using Jordan-Chevalley decompositions.

Chapter 2 is devoted to the study of separable algebras over commutative rings with the purpose of establishing the equivalence of this concept with the classical

one for algebras over fields. This equivalence will allow us, later in Chapter 3, to recover the classical version of the Wedderburn-Malcev Theorem. The first three sections introduce the concept of separable algebras. The fourth one proves that typical algebraic constructions are preserved by separability: products and tensor products of algebras, taking quotients, extending scalars, etc. Section 5 studies separable algebras over semisimple rings, paving the way for section 6 in which we establish the connection between separable and classical separable algebras.

Chapter 3 studies extensions of algebras and proves a general version of the Wedderburn-Malcev Theorem. This is done by translating to our setting the lovely paper of Hochschild [45]. We perform this task in the last two sections, while the first one is devoted to establish the connection between two concepts which are later used interchangeably: the classical Hochschild cohomology modules of an algebra and the modern analogous defined in homological algebra.

The last section of each of the last three chapters contain examples and counterexamples pertinent to the material covered.

Chapter 0

Preliminaries

The purpose of this chapter is to introduce basic concepts, conventions and notation that are assumed to be known by the reader. We include them for the sake of completeness. General references are: Rotman [79], chapter 2 for the first section and Pierce [82], chapters 2,3 and 4 for the second section.

We assume that the reader is familiar with the basic notions of rings, modules and tensor products. This can be found, for instance, in Hungerford [74], chapters III and IV.

To understand some of the examples, a rudimentary knowledge of localization of commutative rings is needed. Atiyah-Macdonald [69], chapter 3, provides an adequate account of this.

We adopt a few conventions valid throughout:

Implicit in our definition of a ring is the existence of a multiplicative identity. Ring homomorphisms are always one-preserving.

We think of modules as representations of rings. It follows that the zero ring admits only the zero abelian group as module and that the prefixes left and right are redundant for modules over commutative rings.

If R is a commutative ring, an R-algebra is an R-module A with an R-bilinear multiplication μ. If μ is associative then we say A is associative and if μ admits an identity element then A is called unital.

Thus an associative unital algebra A is a ring with an R-bilinear multiplication or, equivalently, a ring with a central ring homomorphism $\rho\colon R \to A$. All algebras in this chapter will be associative and unital. Given any left or right A-module M any reference to the R-module structure of M will mean the one inherited from A by means of ρ. Any ring is an algebra over its center.

Specific assumptions will be made in each chapter and/or section.

0.1 Exactness

Given a commutative ring R and an R-algebra A, the category whose objects are all left A-modules and whose morphisms are homomorphisms of left A-modules will be denoted by $A-Mod$. The analogous category for right A-modules will be denoted by $Mod-A$.

Recall that $Hom_A(M,N)$ is an R-module whenever M and N are left A-modules. If A' is also an algebra over a commutative ring R' then we say that a functor $F\colon A-Mod \to A'-Mod$ is **additive** if $F(f+g) = F(f) + F(g)$ for any f, g in $Hom_A(M,N)$. In this case F sends the zero module into the zero module.

In this section we only consider additive functors. Assume now that F is covariant.

Definition 1. F is said to be **left exact** if exactness of $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ in $A-Mod$ implies that of $0 \to F(A) \xrightarrow{F(\alpha)} F(B) \xrightarrow{F(\beta)} F(C)$ in A'-Mod.
F is called **right exact** if exactness of $A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ in A-Mod implies that of $F(A) \xrightarrow{F(\alpha)} F(B) \xrightarrow{F(\beta)} F(C) \to 0$ in $A'-Mod$.

We say that F is **exact** if F is both left and right exact.

Proposition 1. *The following conditions are equivalent:*
(i) F is exact.
(ii) F preserves all exact sequences.
(iii) F preserves all exact sequences of three modules $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$.
(iv) F preserves all short exact sequences $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$.
(v) F is left exact and preserves epimorphisms.
(vi) F is right exact and preserves monomorphisms.

The next two examples are typical.

Example 1. Fix a left A-module M. Then $Hom_A(M,-)\colon A-Mod \to R-Mod$ is left exact. Here $Hom_A(M,-)$ is the functor which sends each left A-module N into the R-module $Hom_A(M,N)$ and each homomorphism of left A-modules $f\colon N \to N'$ into the homomorphism of R-modules $f^*\colon Hom_A(M,N) \to Hom_A(M,N')$

defined by $Hom_A(M,N) \ni g \to fg \in Hom_A(M,N')$.

Example 2. Fix a right A-module M. Then $M \bigotimes_A : A-Mod \to R-Mod$ is right exact. Here $M \bigotimes_A$ is the functor which sends each left A-module N into the R-module $M \bigotimes_A N$ and each homomorphism of left A-modules $f: N \to N'$ into the homomorphism of R-modules $1_M \otimes f: M \bigotimes_A N \to M \bigotimes_A N'$.

These functors are not exact in general, as the following examples show.

Example 3. $Hom_{\mathbf{Z}}(\mathbf{Q}, -): \mathbf{Z}-Mod \to \mathbf{Z}-Mod$ is not exact. To see this we show that $Hom_{\mathbf{Z}}(\mathbf{Q}, -)$ does not preserve epimorphisms.

Indeed, let F be any free abelian group having a quotient isomorphic to $\mathbf{Q}$. Then the epimorphism $f: F \to \mathbf{Q}$ is not preserved by $Hom_{\mathbf{Z}}(\mathbf{Q}, -)$ since there is no $g \in Hom_{\mathbf{Z}}(\mathbf{Q}, F)$ satisfying $fg = 1_{\mathbf{Q}}$. This is so because $Hom_{\mathbf{Z}}(\mathbf{Q}, F) = (0)$.

Example 4. Let M be an R-module having a non-zero element m killed by some $0 \neq r \in R$ which is not a zero-divisor. Then $M \bigotimes_R$ is not exact. To see this we show that $M \bigotimes_R$ does not preserve monomorphisms.

Indeed, let $S = \{1, r, r^2, \cdots\}$. Then $R \to S^{-1}R$ is a monomorphism but $M \bigotimes_R R \to M \bigotimes_R S^{-1}R$ is not since $0 \neq m \otimes 1 \in M \bigotimes_R R$ but $0 = m \otimes 1 \in M \bigotimes_R S^{-1}R$.

A particular case of this occurs when $R = \mathbf{Z}$ and M is an abelian group with torsion.

Modules which do not give rise to the pathologies of Examples 3 and 4 deserve a name, which is now given.

Definition and Proposition 2. *A left A-module M is called* **projective** *if it satisfies the following equivalent conditions:*

(i) $Hom_A(M, -)$ is exact.

(ii) $Hom_A(M, -)$ preserves epimorphisms.

(iii) M is isomorphic to a direct summand of a free left A-module.

(iv) (Dual Basis Lemma) There is a family $(f_i, m_i)_{i \in I}$ where the f_i's are in $Hom_A(M, A)$, the m_i's are in M and they satisfy:

(a) For each $m \in M$ the set $I_m = \{i \in I | f_i(m) \neq 0\}$ is finite.

(b) For each $m \in M$ we have $m = \sum_{i \in I_m} f_i(m) m_i$.

The family $(f_i, m_i)_{i \in I}$ is called a **dual basis** for M. Example 3 shows that the $\mathbf{Z}$-module $\mathbf{Q}$ is not projective. Free modules are always projective. The next typical example shows a non-free projective module.

Example 5. $\mathbf{Z}_6 = \mathbf{Z}_2 \bigoplus \mathbf{Z}_3$ as $\mathbf{Z}_6$-modules. Hence $\mathbf{Z}_2$ and $\mathbf{Z}_3$ are projective $\mathbf{Z}_6$-modules.

Definition and Proposition 3. A right A-module M is **flat** if it satisfies the following equivalent conditions:

(i) $M \bigotimes_A$ is exact.

(ii) $M \bigotimes_A$ preserves monomorphisms.

(iii) If N is a left A-module and N' is a finitely generated submodule of N then $M \bigotimes_A N' \to M \bigotimes_A N$ is injective.

Free, and more generally, projective modules are always flat. The next examples show that flat modules need not be projective.

Example 6. If D is a principal ideal domain (PID) and M a D-module then M is flat if and only if M is torsion free.

A subset S of R is called **multiplicative** if $1 \in S$ and the product of any two elements of S lies in S.

Example 7. $\mathbf{Q}$ is a flat $\mathbf{Z}$-module. More generally, if a subset S of the commutative ring R is multiplicative then $S^{-1}R$ is a flat R-module. Indeed, the functors S^{-1}, $S^{-1}R \bigotimes_R$: $R\text{-}Mod \to S^{-1}R\text{-}Mod$ are naturally isomorphic and S^{-1} is exact.

An excellent account of flatness can be found in Knight [71].

0.2. Semisimplicity

In this section A will denote simply a ring.

Definition and Proposition 1. *A left A-module M is* **simple** *if it satisfies any*

of the following equivalent conditions:

(i) $M \neq (0)$ *and* M *has no proper non-trivial submodules.*

(ii) $M \neq (0)$ *and if* $f\colon M \to N$ *is a homomorphism of left* A*-modules then* f *is injective or identically zero.*

(iii) $M \neq (0)$ *and any non-zero element of* M *generates* M*.*

(iv) There is maximal left ideal I *of* A *such that* $A/I \simeq M$*.*

The ideal I can be taken to be the **annihilator** of any generator of M and need not be unique. By annihilator we mean the following:

Definition 2. *If* M *is a left* A *module,* M_1 *a submodule and* M_2 *a subset of* M*, denote by* (M_1, M_2) *the left ideal of* A *consisting of all* a *satisfying* $aM_2 \subset M_1$*. The left ideal* $(0, M_2)$ *is called the annihilator of* M_2*. It is denoted by* $An_A(M_2)$*.*

In general (M_1, M_2) is not an ideal of A, but this is the case if M_2 is a submodule of M. Observe that the annihilator of M is nothing but the kernel of the representation of A in M.

If A is commutative I is unique. Indeed, $I = \mathrm{An}_A(M) = \mathrm{An}_A(m)$ for any $0 \neq m \in M$.

Example 1. Let Δ be a division ring, $n > 1$ and $A = M_n(\Delta)$. Let M_k and N_k be the left ideals of A respectively consisting of all those matrices whose columns other that the $k-th$ are are 0 and all those matrices whose $k-th$ column is 0, $k = 1, \cdots, n$. Then:

(i) Each M_k is a simple left A-module.

(ii) $A/N_k \simeq M_j$ for all $1 \leq j, k \leq n$, showing that the ideal I is not unique.

(iii) The M_k's are all isomorphic.

(iv) $A = M_1 \bigoplus \cdots \bigoplus M_n$.

(v) A has no proper non-trivial ideal.

Properties (iv) and (v) characterise certain type of modules and rings, which we now define.

Definition and Proposition 2. *A left* A*-module* M *is* **semisimple** *if it satisfies*

any of the following equivalent conditions:

(i) M is the sum of simple submodules.

(ii) M is the direct sum of simple submodules.

(iii) Every submodule of M is a direct summand of M.

(iv) Every short exact sequence of left A modules $0 \to N \to M \to N' \to 0$ splits.

(v) Every cyclic submodule of M is the sum of simple submodules.

The ring A itself is said to be left semisimple if its left regular representation turns it into a semisimple left A-module. We say that A is simple if $A \neq (0)$ and A has no proper non-zero ideals.

The definition of right semisimplicity of modules and rings is done along similar lines.

Example 1 shows that $M_n(\Delta)$ is left semisimple and simple. Using rows instead of columns we see that $M_n(\Delta)$ is also right semisimple. This is not casual (see Theorem 1 below).

Example 2. Every left module over a division ring is semisimple.

Example 3. Let $\mathcal{N} = \{N_i : i \in I\}$ be a set of representatives of the isomorphism classes of simple left A-modules (I is a set due to Proposition 1(iv)). Let M be a semisimple left A-module and for each $i \in I$ let $M(i)$ be the sum of all submodules of M isomorphic to N_i. Then:

(i) M is the direct sum of the $M(i)$'s.

(ii) The cardinal number $\alpha(M)_i$ of of simple submodules of M isomorphic to N_i appearing in any decomposition of M as the direct sum of simple submodules is an invariant of the module M.

For instance, if $A = \mathbf{Z}$ and $\mathcal{N} = \{\mathbf{Z}_p : p$ is a positive rational prime$\}$ then $\alpha(M)_p$ is the dimension of $M(p)$ over the field $\mathbf{Z}_p$. Moreover, if N is also semisimple then $M \otimes_{\mathbf{Z}} N$ is semisimple as well and $\alpha(M \otimes_{\mathbf{Z}} N)_p = \alpha(M)_p.\alpha(N)_p$.

We now turn to semisimplicity of rings.

Definition 3. The **Jacobson radical** $J(M)$ of a left A-module M is the inter-

section of all its maximal submodules.

Of course, M might not have any maximal submodules in which case we agree that $J(M) = M$. An important case when M does have a maximal submodule occurs when M is finitely generated (and non-zero).

Example 4. A module M over a PID D is divisible if $dM = M$ for every $0 \neq d \in D$. If D is a field M is obviously divisible. If D is not a field then M is divisible if and only if $J(M) = M$. Thus the only finitely generated divisible D-module is the zero module.

Definition 4. The Jacobson radical $J(A)$ of the ring A is the the intersection of all maximal left ideals of A.

Thus $J(A)$ is the Jacobson radical of A viewed as a left module over itself. This lack of symmetry is only apparent. Indeed, $J(A)$ is also the intersection of all maximal right ideals of A. In particular $J(A)$ is an ideal of A.

Since A is generated by 1 as a left A-module, A does have maximal left ideals (if $A \neq (0)$).

Example 5. $J(M_n(A)) = M_n(J(A))$.

Example 6. If $\mathbb{K}$ is a field and $\mathbb{K}[[t]]$ is the ring of formal power series over $\mathbb{K}$ then $J(\mathbb{K}[[t]]) = (t)$.

Recall that A is **left artinian** if every non-empty collection of left ideals of A has a minimal member. For instance, a finite dimensional associative and unital algebra over a field is always left artinian.

Proposition 5. *The Jacobson radical of a left artinian ring A is nilpotent. Moreover, if A is also commutative its Jacobson radical consist of all nilpotent elements of A.*

Theorem 1. *Let A be a non-zero ring. The following conditions are equivalent:*
(1) A is left semisimple.
(2) A is left artinian and $J(A) = (0)$.

(3) Every left A-module is projective.

(4) Every short exact sequence of left A-modules splits.

(5) Every left A-module is semisimple.

(6) For every ring A', every additive functor $F\colon A-Mod \to A'-Mod$ is exact.

(7) A is the direct product of a finite number of simple left artinian rings.

(8) (Artin-Wedderburn) A is the direct product of a finite number of full matrix rings over division rings.

(9) A is right semisimple.

Chapter 1

Jordan-Chevalley decomposition

This chapters deals with endomorphisms acting on a (possibly infinite dimensional) linear space in general and with Jordan-Chevalley decompositions in particular. This has been motivated by Chapter 7.1 in Moody-Pianzola [to appear] and Bourbaki [90].

1.1. Modules over a principal ideal domain

Let D be a PID, $\mathcal{P}$ a set of representatives of the primes in D, M a D-module and $p \in \mathcal{P}$ (the choice of $\mathcal{P}$ is immaterial in what follows).

The following (fully invariant) submodules of M arise quite naturally: $T(M)$, M^p, the **socle** $Soc(M)$ of M and M_p consisting of those elements of M respectively killed by some non-zero element of D, some power of p, a product of distinct primes in $\mathcal{P}$ and p.

M is respectively called **elementary**, **p-primary, torsion** and **bounded** if $Soc(M) = M$, $M = M^p$, $T(M) = M$ and $An_D(M) \neq (0)$.

The **spectrum** $spec(M)$ of M consists of all $q \in \mathcal{P}$ such that $M^q \neq (0)$.

Proposition 1. *For each $q \in \mathcal{P}$ let $N(q)$ be a q-primary submodule of M and let N be a submodule of $\sum_{q\in\mathcal{P}} N(q)$. Then:*
(i) the sum $\sum_{q\in\mathcal{P}} N(q)$ is direct.
(ii) $N = \bigoplus_{q\in\mathcal{P}}(N \cap N(q))$.

Proof. Let $n \in N$. Then $n = n_{q_1} + \cdots + n_{q_l}$ for some $l \in \mathbb{N}$, $q_i \in \mathcal{P}$ and $n_{q_i} \in N(q_i)$. We know that $q_i^{k_i} n_{q_i} = 0$ for some $k_i \in \mathbb{N}$ and each $1 \leq i \leq l$.

If $l = 1$ then $n = n_{q_1} \in N$. If $l > 1$ take any i, $1 \leq i \leq l$, and let $p_i = \prod_{j\neq i} q_j^{k_j}$. Then $p_i n \in N$ and $p_i n_{q_j} = 0 \in N$ for all $j \neq i$. Hence $p_i n_{q_i} \in N$ as well, and since $(p_i, q^{k_i}) = 1$ we see at once that $n_{q_i} \in N$.

We have shown that $N = \sum_{q\in\mathcal{P}} (N \cap N(q))$. Taking $N = (0)$ in the foregoing argument we obtain (i). Combining these two facts we finally get (ii). ♣

Theorem 1. *(primary decomposition)*

(i) M is torsion iff $M = \bigoplus_{q\in\mathcal{P}} M^q$.

(ii) If M is torsion and $M = \bigoplus_{q\in\mathcal{P}} N(q)$, where each $N(q)$ is q-primary, then $N(q) = M^q$ for all $q \in \mathcal{P}$.

Proof.

(i) We only need to show that if M is torsion then $M = \sum_{q\in\mathcal{P}} M^q$. Take any $m \in M$. Then m is killed by some element of the form $q_1^{k_1} \cdots q_l^{k_l}$. If $l = 1$ then $m \in M^{q_1}$. If $l > 1$ let $p_i = \prod_{j\neq i} q_j^{k_j}$ for each $1 \leq i \leq l$. Since the p_i's are coprime $1 = d_1p_1 + \cdots + d_lp_l$ for some $d_i \in D$. Hence $m = d_1p_1m + \cdots + d_lp_lm$ and $d_ip_im \in M^{q_i}$ for each $1 \leq i \leq l$.

(ii) $N(q) \subset M^q$ is clear. Now $M^q = \bigoplus_{q'\in\mathcal{P}}(M^q \cap N(q')) = M^q \cap N(q)$ by Proposition 1. Thus $M^q \subset N(q)$. ♣

Proposition 2. *Being semisimple and elementary are equivalent conditions for D-modules if and only if D is not a field.*

Proof. If D is a field then all non-zero D-modules are semisimple and not elementary.

Suppose now that D is not a field. Then D is not semisimple since *every semisimple integral domain R is a field.* A simple proof of this fact is the following.

Pick any non-zero $r \in R$. Look at R as a left module over itself in the obvious manner. Since R is left semisimple the left ideal (r) is complemented in R, that is $R = (r) \bigoplus I$ for some left ideal I if R. This decomposition of R into the direct sum of two of its submodules must come from an R-linear projection of R. This means that there is an R-linear endomorphism ρ such that: $\rho^2 = \rho$ and $\rho(R) = (r)$.

But $\rho(1) = \rho^2(1) = \rho(\rho(1).1) = \rho(1)^2$ is telling us that $\rho(1)$ is an idempotent in R. Since R has no zero divisors $\rho(1)$ is 1 or 0. We now use the facts that $\rho(R) = (r)$ and $r \neq 0$ to rule out the case $\rho(1) = 0$. Therefore ρ is the identity on R, and so (r)=R. Thus, r is left invertible. R being commutative the assertion is proven.

Now given a semisimple D-module M, pick any $m \in M$. The homomorphism of D-modules $D \ni d \xrightarrow{Y_m} dm \in Dm$ is not injective because D is not semisimple and Dm is. Thus, $m \in T(M)$. We have shown that M is torsion.
To see that M is elementary assume first that M is p-primary. Since Dm is semisimple the kernel of Y_m is necessarily generated by (p) or (1). Hence, M is elementary. The general case now follows from the last Theorem.

Conversely, assume that M is elementary. It suffices to show that each primary component of M is semisimple. But every cyclic submodule of a primary component of M is (0) or simple. The result thus follows. ♣

Proposition 3. *Let $d \in D$. The map L_d defined by $M \ni m \mapsto dm \in M$ is an automorphism of $T(M)$ iff q does not divide d, whenever $q \in spec(M)$.*

Proof. The statement being vacuous when M is torsion free, we assume that $T(M) \neq (0)$. Since the primary components of $T(M)$ are fully invariant we can use the last Theorem to reduce the problem to the case $T(M) = M^p$. In this case we see at once that L_d is injective in $T(M)$ if and only if p does not divides d. Moreover if p is coprime to d then given $m \in T(M)$ we have $p^k m = 0$ for some $k \in \mathbb{N}$ and $1 = p^k h_1 + dh_2$ for some $h_1, h_2 \in D$. Hence $L_d(h_2 m) = m$, showing that L_d is surjective. ♣

1.2. Various types of endomorphisms

Let $\mathbb{K}$ be a field. If $\mathbf{V}$ is a $\mathbb{K}$-space and $x \in End_{\mathbb{K}}(\mathbf{V})$ we can make $\mathbf{V}$ into a $\mathbb{K}[t]$-module $\mathbf{V}(x)$ via the unique $\mathbb{K}$-algebra morphism $\mathbb{K}[t] \longrightarrow End_{\mathbb{K}}(\mathbf{V})$ extending $t \to x$; thus $p(t).v = p(x)(v)$ when $p(t) \in \mathbb{K}[t]$ and $v \in \mathbf{V}$.

In this setting, $\mathcal{P}$ is the collection of all irreducible monic polynomials in $\mathbb{K}[t]$, the primary component $\mathbf{V}^{t-a}(x)$, $a \in \mathbb{K}$, denoted simply by $\mathbf{V}^a(x)$ is the **generalised eigenspace** corresponding to a while $\mathbf{V}_{t-a}(x)$, denoted by $\mathbf{V}_a(x)$ is the **eigenspace corresponding** to a.

We will refer to $spec(\mathbf{V}(x))$ as the spectrum of x and will denote it by $spec(x)$.

x is said to be **algebraic** if $\mathbf{V}(x)$ is bounded, **semisimple** if $\mathbf{V}(x)$ is semisimple,

locally finite if $\mathbb{V}(x)$ is torsion, **locally nilpotent** if $\mathbb{V}(x) = \mathbb{V}^o(x)$, **cyclic** if $\mathbb{V}(x)$ is cyclic, **diagonalizable** if $\mathrm{V}(x) = \bigoplus_{a\in\mathbb{K}} \mathrm{V}_a(x)$, **triangularizable** if $\mathbb{V}$ has a totally ordered basis B such that $x(v) \in \sum_{u\leq v} \mathbb{K}u$ for all $v \in B$ and **Split** if $\mathbb{V}(x) = \bigoplus_{a\in\mathbb{K}} \mathbb{V}^a(x)$.

We note that a submodule $\mathbb{W}$ of $\mathbb{V}(x)$ is nothing but an x-invariant subspace of $\mathbb{V}$. The x-invariant subspace of $\mathbb{V}$ generated by $v \in \mathbb{V}$ will be denoted be $Z(x, v)$.

Recall that if $\mathbb{U}$ is merely a subset of $\mathbb{V}$ then $(\mathbb{W}, \mathbb{U})$ denotes the ideal of $\mathbb{K}[t]$ consisting of those p satisfying $p(x)(u) \in W$ for all $u \in \mathbb{U}$. An extreme case would be that $(\mathbb{W}, \mathbb{U}) = (0)$. The remaining cases give rise to the following:

Definition 1. Let $\mathcal{P}' = \mathcal{P} \cup \{1\}$. Suppose that $(\mathbb{W}, \mathbb{U})$ is a non-zero ideal and let g be the unique generator of $(\mathbb{W}, \mathbb{U})$ written as a product of elements of $\mathcal{P}'$.
(i) If $\mathbb{U} = \{v\}$ then g is called the x-**conductor** of v into $\mathbb{W}$.
(ii) The x-conductor $p_{x,v}$ of v into (0) is the **minimal polynomial** of v.
(iii) If $\mathbb{U} = \mathbb{V}$ and $\mathbb{W} = (0)$ then g is the minimal polynomial of x, denoted by p_x.

By definition the minimal polynomial of the zero vector and x acting on the zero space are both 1. We will denote $(\mathbb{W}, \{v\})$ by $(\mathbb{W}, v)$ and $((0), \mathbb{U})$ by $(0, \mathbb{U})$. The following Lemma explains when Definition 1 can be applied:

Lemma 1.
(i) $(\mathbb{W}, v) \neq (0)$ *iff* $Z(\tilde{x}, \tilde{v})$ *is finite dimensional over* $\mathbb{K}$, *where* $\tilde{x}$ *is the endomorphism induced by* x *on* $\mathbb{V}/\mathbb{W}$ *and* $\tilde{v} = v + \mathbb{W}$.
(ii) $(0, v) \neq (0)$ *iff* $Z(x, v)$ *is finite dimensional over* $\mathbb{K}$.
(iii) $(0, \mathbb{V}) \neq (0)$ *iff* $\mathbb{V}(x)$ *is not a faithful* $\mathbb{K}[t]$*-module iff* x *is algebraic.*

Proof.
(i) Since $(\mathbb{W}, v) = (0, v + \mathbb{W})$ (i) follows from (ii).
(ii) If $(0, v) \neq (0)$ then $p \in (0, v)$ for some p of degree $k \geq 1$. Thus $v, \ldots, x^{k-1}(v)$ generate $Z(x, v)$. Conversely if $Z(x, v)$ is finite dimensional then $x^k(v)$ is a linear combination of $v, \ldots, x^{k-1}(v)$ for some $k \geq 1$. We then use this linear combination to construct a non-zero p in $(0, v)$.

(iii) This is a restatement of the definitions. ♣

We translate some of the results of Section 1.1 into the following:

Proposition 1.

(i) x is semisimple iff x is locally finite the minimal polynomial of every vector in $\mathbb{V}$ is a product of distinct elements of $\mathcal{P}'$ iff $\mathbb{V}(x) = \bigoplus_{p\in\mathcal{P}} \mathbb{V}_p(x)$. In particular if x is semisimple then x is locally finite.

(ii) x is locally finite iff $\mathbb{V}(x) = \bigoplus_{p\in\mathcal{P}} \mathbb{V}^p(x)$ iff $dim_{\mathbb{K}} Z(x,v) < \infty$ for very $v \in \mathbb{V}$. In particular, if x is algebraic then x is semisimple iff its minimal polynomial is a product of distinct elements of $\mathcal{P}'$.

(iii) x is semisimple and locally nilpotent iff $x = 0$.

Proof.

(i) It follows at once from Propositions 1 and 2 of Section 1.1.

(ii) It follows from Theorem 1.1.1 and Lemma 1(ii).

(iii) If x is semisimple and locally nilpotent then the minimal polynomial of a non-zero $v \in \mathbb{V}$ is a product of distinct primes in $\mathbb{K}[t]$ and t^n, for some $n \in \boldsymbol{N}$, at the same time. Hence, it is just t, and so $x = 0$. ♣

1.3. Extension of scalars

Let $\mathcal{C}_{\mathbb{K}}$ be the category whose objects are all pairs $(\mathbb{V}, x)$, where $\mathbb{V}$ is a $\mathbb{K}$-space and $x \in End_{\mathbb{K}}(\mathbb{V})$, a morphism from $(\mathbb{V}, x)$ to another such a pair $(\mathbb{W}, y)$ being a $\mathbb{K}$-linear map $\varphi \in Hom_{\mathbb{K}}(\mathbb{V}, \mathbb{W})$ satisfying $y\varphi = \varphi x$.

The functor $\mathcal{C}_{\mathbb{K}} \longrightarrow \mathbb{K}[t]$-Mod, defined:

$$\begin{array}{ccc} (\mathbb{V}, x) & \longrightarrow & \mathbb{V}(x) \\ \varphi & \longrightarrow & \varphi \end{array}$$

can be reversed to obtain a functor $\mathbb{K}[t]$-Mod $\longrightarrow \mathcal{C}_{\mathbb{K}}$ as follows:

$$\begin{array}{ccc} \mathbb{V} & \longrightarrow & (\mathbb{V}, x) \\ \varphi & \longrightarrow & \varphi \end{array}$$

where $x(v) = t.v$ for all $v \in \mathbb{V}$, obtaining isomorphic categories.

From now on $\mathbb{F}$ will denote a field extension of $\mathbb{K}$. We extend scalars to $\mathbb{F}$ via the functor $\mathbb{K}$-Mod $\longrightarrow$ $\mathbb{F}$-Mod (*):

$$\begin{array}{ccc} \mathbf{V} & \longrightarrow & \mathbf{V}_{\mathbb{F}} = \mathbb{F} \bigotimes_{\mathbb{K}} \mathbf{V} \\ y \in Hom_{\mathbb{K}}(\mathbf{V}, \mathbf{W}) & \longrightarrow & y_{\mathbb{F}} = 1_{\mathbb{F}} \otimes y \in Hom_{\mathbb{F}}(\mathbf{V}_{\mathbb{F}}, \mathbf{W}_{\mathbb{F}}) \end{array}$$

This is a $\mathbb{K}$-linear faithful functor, that is, if $y, z \in Hom_{\mathbb{K}}(\mathbf{V}, \mathbf{W})$ and $k \in \mathbb{K}$ then $(ky + z)_{\mathbb{F}} = ky_{\mathbb{F}} + z_{\mathbb{F}}$ and $y_{\mathbb{F}} = z_{\mathbb{F}}$ implies $y = z$.

We use this construction to get a functor $\mathcal{C}_{\mathbb{K}} \longrightarrow \mathcal{C}_{\mathbb{F}}$:

$$\begin{array}{ccc} (\mathbf{V}, x) & \longrightarrow & (\mathbf{V}_{\mathbb{F}}, x_{\mathbb{F}}) \\ \varphi & \longrightarrow & \varphi \otimes 1_{\mathbb{F}} \end{array}$$

finally arriving to:

Note 1. *There are two ways to reach $\mathbb{F}[t]$-Mod from $\mathcal{C}_{\mathbb{K}}$, namely*

$$\begin{array}{ccc} \mathcal{C}_{\mathbb{K}} & \longrightarrow & \mathbb{K}[t]\text{-}Mod \\ \downarrow & & \downarrow \\ \mathcal{C}_{\mathbb{F}} & \longrightarrow & \mathbb{F}[t]\text{-}Mod \end{array}$$

which are naturally isomorphic (the right vertical arrow, extension of scalars from $\mathbb{K}[t]$ to $\mathbb{F}[t]$, is defined mutatis mutandis as in (*)).

It will also be useful to know that:

Note 2. *$\mathcal{C}_{\mathbb{K}} \longrightarrow \mathcal{C}_{\mathbb{F}} \longrightarrow \mathcal{C}_{\mathbb{L}}$ and $\mathcal{C}_{\mathbb{K}} \longrightarrow \mathcal{C}_{\mathbb{L}}$ are naturally isomorphic for any field extension $\mathbb{L}$ of $\mathbb{F}$.*

1.4. Eigenvalues and characteristic roots

We define and compare the concepts of eigenvalue and characteristic root in the infinite dimensional setting.

Fix an algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$ and declare a $\lambda \in \overline{\mathbb{K}}$ to be an eigenvalue of x if λ is an eigenvalue of $x_{\overline{\mathbb{K}}}$, collecting all such λ's in $E(x) \subset \overline{\mathbb{K}}$, and to be a characteristic root of x if λ is a root of the minimal polynomial of some vector of $\mathbf{V}$, gathering all such λ's in $CR(x) \subset \overline{\mathbb{K}}$. Nicely enough, $E(x) = CR(x)$. We divide the proof in several parts.

Lemma 1. *$\mathbf{V}(x)$ is torsion free iff $\mathbf{V}_{\mathbb{F}}(x_{\mathbb{F}})$ is torsion free.*

Proof. Sufficiency is clear. For the necessity we first suppose that $\mathbb{F}$ is algebraically closed. If $\mathbf{V}_{\mathbb{F}}(x_{\mathbb{F}})$ has torsion then $x_{\mathbb{F}}$ must then have an eigenvalue $\lambda \in \mathbb{F}$. Let $\mathcal{F}$ be a basis of $\mathbb{F}$ over $\mathbb{K}$. If $u \in \mathbf{V}_{\mathbb{F}}$ is an eigenvector of $x_{\mathbb{F}}$ corresponding to λ, then $u = \sum_{i=1}^{n} f_i \otimes v_i$ for unique (up to a simultaneous reordering) sequences $(f_i)_{1 \leq i \leq n}$ of distinct elements of $\mathcal{F}$ and $(v_i)_{1 \leq i \leq n}$ of non-zero vectors of $\mathbf{V}$. Choose $m \gg 0$ so that $\lambda f_j = \sum_{i=1}^{m} a_{ij} f_i$, where $1 \leq j \leq n$ and $a_{ij} \in \mathbb{K}$. Thus, $\sum_{i=1}^{n} f_i \otimes x(v_i) = x_{\mathbb{F}}(u) = \lambda u = \sum_{j=1}^{n} \lambda f_j \otimes v_j = \sum_{j=1}^{n} (\sum_{i=1}^{m} f_i \otimes a_{ij} v_j) = \sum_{i=1}^{m} f_i \otimes (\sum_{j=1}^{n} a_{ij} v_j)$. Hence $x(v_i) = \sum_{j=1}^{n} a_{ij} v_j$ for each $1 \leq i \leq n$, showing that the $\mathbb{K}$-space generated by $v_1, \cdots, v_n$ is x-invariant, contradicting the fact that $\mathbf{V}(x)$ is torsion free.

The general case follows from above and Note 1.3.2. ♣

Lemma 2. *If $\mathbf{W} \subset \mathbf{V}$ is an x-invariant subspace then the $\mathbb{F}[t]$-modules $(\mathbf{V}/\mathbf{W})_{\mathbb{F}}$ and $\mathbf{V}_{\mathbb{F}}/\mathbf{W}_{\mathbb{F}}$ are isomorphic.*

Proof The sequence of $\mathbb{K}[t]$-modules $0 \longrightarrow \mathbf{W} \longrightarrow \mathbf{V} \longrightarrow \mathbf{V}/\mathbf{W} \longrightarrow 0$ is exact. Applying $\mathbb{F}[t] \bigotimes_{\mathbb{K}[t]}$— we get an exact sequence of $\mathbb{F}[t]$-modules, which is what we want by Note 1.3.1 ($\mathbb{F}[t]$ is a flat $\mathbb{K}[t]$-module, see Chapter 0, Example 6). ♣

Proposition 1. $T(\mathbf{V}_{\mathbb{F}}(x_{\mathbb{F}})) = T(\mathbf{V}(x))_{\mathbb{F}}$.

Proof. By the preceding results $(\mathbf{V}/T(\mathbf{V}))_{\mathbb{F}} \simeq \mathbf{V}_{\mathbb{F}}/T(\mathbf{V})_{\mathbb{F}}$ is torsion free, so that $T(\mathbf{V}_{\mathbb{F}}(x_{\mathbb{F}})) \subset T(\mathbf{V}(x))_{\mathbb{F}}$. The other inclusion is obvious. ♣

Note 1. *If $v \in \mathbf{V}$ then $v \in T(\mathbf{V}(x))$ iff $1 \otimes v \in T(\mathbf{V}_{\mathbb{F}}(x_{\mathbb{F}}))$. Moreover, in this case*

(A) $$p_{x,v} = p_{x_{\mathbb{F}}, 1 \otimes v}.$$

Corollary 1. $E(x) = CR(x)$.

Proof. We first note this is true when x is locally finite. In this case,

$$CR(x) = CR(x_{\overline{\mathbb{K}}}) = E(x_{\overline{\mathbb{K}}}) = E(x).$$

All equalities are clear excepting the first one, while $CR(x) \subset CR(x_{\overline{\mathbb{K}}})$ follows from (A). Since $T = \{1 \otimes v | v \in \mathbf{V}\}$ spans $\mathbf{V}_{\overline{\mathbb{K}}}$, the minimal polynomial of any non-zero vector of $\mathbf{V}_{\overline{\mathbb{K}}}$ divides a product of minimal polynomial of vectors of T, and hence of $\mathbf{V}$ (we are using that x is locally finite and (A) at this point). This shows $CR(x_{\overline{\mathbb{K}}}) \subset CR(x)$.

The general case follows now from above and the proposition. Indeed, $E(x) = E(x_{\overline{\mathbb{K}}}) = E(x_{\overline{\mathbb{K}}}|_{T(\mathbf{V}_{\overline{\mathbb{K}}})}) = E(x_{\overline{\mathbb{K}}}|_{T(\mathbf{V})_{\overline{\mathbb{K}}}}) = E((x|_{T(\mathbf{V})})_{\overline{\mathbb{K}}}) = E(x|_{T(\mathbf{V})}) = CR(x|_{T(\mathbf{V})}) = CR(x)$. ♣

Corollary 1 extends the locally finite case, appeared in Caserta [91].

Corollary 2. *x is locally finite iff $x_{\mathbb{F}}$ is locally finite.*

Proof. Immediate consequence of Proposition 1. ♣

1.5. Semisimplicity and extension of scalars

A diagonalizable endomorphism is semisimple and has all its eigenvalues in the ground field. The converse is true as shown in the

Proposition 1. *The following conditions are equivalent:*

(i) x is diagonalizable.

(ii) x is locally finite and the minimal polynomial of every non-zero vector of $\mathbf{V}$. splits into different monic linear factors in $\mathbb{K}[t]$.

(iii) x is semisimple and $E(x) \subset \mathbb{K}$

(iv) x is semisimple and every irreducible submodule of $\mathbf{V}(x)$ is a one dimensional subspace of $\mathbf{V}$.

Proof.

(i)⇒(ii) It follows from the definitions.

(ii)⇒(iii) Use Proposition 1.2.1(i) and Corollary 1.4.1.

(iii)⇒(iv) $p_{x,v}$ is monic linear for any $\mathbb{K}[t]$-generator v of an irreducible submodule of $\mathbf{V}(x)$.

(iv)⇒(i) Since x is semisimple, $\mathbf{V}(x) = \bigoplus_{p \in \mathcal{P}} \mathbf{V}_p(x)$. For any non-zero $v \in \mathbf{V}_p(x)$

and $p \in \mathcal{P}$, $Z(x,v)$ is irreducible, so $1 = dim_{\mathbb{K}} Z(x,v) = \deg p$, so p is monic and linear and $\mathbf{V}(x) = \bigoplus_{a \in \mathbb{K}} \mathbf{V}_a(x)$. ♣

Proposition 2. *If $x_{\mathbb{F}}$ semisimple then so is x.*

Proof. Apply the criterion of Proposition 1.2.1(i) and then use Note 1.4.1. ♣

The converse of Proposition 2 is false in general, as shown in the next result. It will be the eigenvalues of x who will decide upon semisimplicity when extending scalars.

We say that x is **absolutely semisimple** if $x_{\mathbb{F}}$ is semisimple for every field extension $\mathbb{F}$ of $\mathbb{K}$ and **separable** if its eigenvalues are separable over $\mathbb{K}$. Thus, x is separable iff the minimal polynomial of every non-zero vector of $T(\mathbf{V}(x))$ is separable over $\mathbb{K}$ (i.e. its irreducible factors have distinct roots in their splitting fields). We have:

Proposition 3. *The following conditions are equivalent:*

(i) x is absolutely semisimple.

(ii) For some extension field $\mathbb{F}$ of $\mathbb{K}$, $x_{\mathbb{F}}$ is diagonalizable.

(iii) x is locally finite and $(p_{x,v}, p'_{x,v}) = 1$ for all non-zero $v \in \mathbf{V}$.

(iv) x is semisimple and $p_{x,v}$ is separable over $\mathbb{K}$ for all non-zero $v \in \mathbf{V}$.

(v) x is semisimple and separable.

Proof.

(i)⇒(ii) $x_{\overline{\mathbb{K}}}$ is semisimple and hence diagonalizable.

(ii)⇒(iii) By the first implication of Proposition 1 $x_{\mathbb{F}}$ is locally finite, and hence so is x by Corollary 1.4.2. Since the second condition of (iii) certainly holds for the non-zero vectors of $\mathbf{V}_{\mathbb{F}}$ we can apply (A) to see that it holds for those in $\mathbf{V}$.

(iii)⇒(iv) Pick any $0 \neq v \in \mathbf{V}$. $p_{x,v}$ is a product of distinct primes in $\mathbb{K}[t]$ and has no repeated roots in $\overline{\mathbb{K}}$ for $(p_{x,v}, p'_{x,v}) = 1$.

(iv)⇒(v) Clear.

(v)⇒(i) Let $\mathbb{F}$ be a field extension of $\mathbb{K}$. By Proposition 1.2.1(i) x is locally finite and then so must be $x_{\overline{\mathbb{F}}}$ by Corollary 1.4.2. By hypothesis $p_{x,v}$ splits into different

monic linear factors in $\overline{\mathbb{F}}[t]$, for any $0 \neq v \in \mathbb{V}$. Since $\{1 \otimes v | v \in \mathbb{V}\}$ spans $\mathbb{V}_{\overline{\mathbb{F}}}$ we use (A) to conclude that $p_{x_{\overline{\mathbb{F}}}, w}$ splits into different monic linear factors in $\overline{\mathbb{F}}[t]$, for any $0 \neq w \in \mathbb{V}_{\overline{\mathbb{F}}}$. Hence $x_{\overline{\mathbb{F}}}$ is diagonalizable by Proposition 1(ii). We now apply Note 1.3.2 and Proposition 2 to see that $x_{\mathbb{F}}$ is semisimple. ♣

The next result will be used implicitly in what follows.

Note 1. *x is algebraic (resp. locally nilpotent) iff $x_{\mathbb{F}}$ is algebraic (resp. locally nilpotent).*

1.6. Jordan-Chevalley decomposition

Definition 1. Let $\mathbb{V}$ be a $\mathbb{K}$-space and $x \in End_{\mathbb{K}}(\mathbb{V})$.

A **Jordan-Chevalley decomposition (JCD)** of x is a pair (s, n) of endomorphisms of $\mathbb{V}$ satisfying:

(i) s is semisimple and n is locally nilpotent.

(ii) $s + n = x$ and $sn = ns$.

We say that the above decomposition is:

(a) **absolute** if s is absolutely semisimple.

(b) **standard** if any x-invariant subspace $\mathbb{U}$ of $\mathbb{V}$ is invariant under s and n and whenever $x|_{\mathbb{U}}$ is algebraic then $s|_{\mathbb{U}}$, $n|_{\mathbb{U}} \in \mathbb{K}[x|_{\mathbb{U}}]$.

We find necessary and sufficient conditions for an endomorphism to have either an absolute or a standard Jordan-Chevalley decomposition. These type of decompositions are shown to be unique.

We will see that JCD need not exist or be unique. However given one, say (s, n), there is no ambiguity in referring to the **semisimple** or **locally nilpotent part** of it due to Note 1.2.1(iii).

Proposition 1.

(i) The sum and product of locally finite commuting endomorphisms y, z is locally finite.

(ii) The sum of locally nilpotent commuting endomorphisms is locally nilpotent and so is the product of a locally nilpotent endomorphisms with any other com-

muting with it.

(iii) If f, n are respectively locally finite and locally nilpotent commuting endomorphism and $x = f + n$ then $\mathbb{V}^p(x) = \mathbb{V}^p(f)$ for all $p \in \mathbb{K}[t]$. In particular:

(a) $CR(x) = CR(f)$.

(b) If $dim_{\mathbb{K}}\mathbb{V} < \infty$ then the characteristic polynomials P of x and Q of f are the same.

(c) If $f = s$ is semisimple then $\mathbb{V}^p(x) = \mathbb{V}^p(s) = \mathbb{V}_p(s)$ for all $p \in \mathbb{K}[t]$.

Proof.

(i) Take any non-zero $v \in \mathbb{V}$. Then $q(z)(v) = 0$ for some monic $q \in \mathbb{K}[t]$ of positive degree $k \in \mathbb{N}$. Thus $\mathbb{U} = \sum_{i=0}^{k-1} Z(y, z^i(v))$ is finite dimensional and y-invariant.

Moreover, if $u \in \mathbb{U}$ then $u = \sum_{i=0}^{k-1} q_i(y)(z^i(v))$ for some $q_i \in \mathbb{K}[t]$. Since [y,z]=0 we have, $z(v) = \sum_{i=0}^{k-1} q_i(y)(z^{i+1}(v))$ and since $z^k(v)$ is a $\mathbb{K}$-linear combination of $v, \cdots, z^{k-1}(v)$ we see that $z(v)$ is in $\mathbb{U}$. It follows that $\mathbb{U}$ is invariant under both $y + z$ and yz.

(ii) The case of the product is immediate. For the other use the binomial law.

(iii) Let $p \in \mathbb{K}[t]$. Since $x - f$ is locally nilpotent and $[x, f] = 0$, we can apply (ii) to see that $h = p(x) - p(f)$ is locally nilpotent. If $v \in \mathbb{V}^p(f)$ then $p^i(f)(v)=h^j(v)=0$, for some $i, j \in \mathbb{N}$. Thus $p^{i+j}(x)(v) = 0$, and so $\mathbb{V}^p(f) \subset \mathbb{V}^p(x)$. The other inclusion is proved similarly.

We have proven x and f have the same spectrum. Since the characteristic roots of an endomorphism are the roots of the polynomials in its spectrum, $CR(x) = CR(f)$ holds.

For the statement about the characteristic polynomials we can assume that $\mathbb{K}$ is algebraically closed. Applying what we just proved we get:
$P = \prod_{a \in \mathbb{K}}(t - a)^{dim_{\mathbb{K}}\mathbb{V}^a(x)} = \prod_{a \in \mathbb{K}}(t - a)^{dim_{\mathbb{K}}\mathbb{V}^a(y)} = Q$ as desired. The last assertion is clear. ♣

Corollary 1. *If (s, n) is a standard JCD of x and $\mathbb{U}$ is an x-invariant subspace of $\mathbb{V}$ such that $x|_{\mathbb{U}}$ is algebraic then we can always chose p and q in $\mathbb{K}[t]$ with no constant term such that $p(x|_{\mathbb{U}}) = s|_{\mathbb{U}}$ and $q(x|_{\mathbb{U}}) = n|_{\mathbb{U}}$.*

Proof. To simplify the notation set $X = x|_{\mathbb{U}}$, $S = s|_{\mathbb{U}}$ and $N = n|_{\mathbb{U}}$. Since $S = X - N$ it suffices to prove the assertion about N. We have $h(X) = N$ for some $h \in \mathbb{K}[t]$ and assume that the constant term of h is different from 0. If the constant term of the minimal polynomial p of X is also different from 0 then we can add to h a suitable multiple of p so that the constant term of the resulting polynomial g is 0. Clearly $g(X) = N$ as well.

We now show that the remaining case, namely that constant term of p is 0 can not happen. Indeed, if t divides p then $\mathbb{U}^0(X) \neq (0)$ and hence $Soc(\mathbb{U}^0(X)) = \ker X \neq (0)$. By Proposition 1(iii) $\mathbb{U}^0(X) = \mathbb{U}^0(S) = \mathbb{U}_0(S)$, that is X and N agree on $\mathbb{U}^0(X)$. If we now pick any $0 \neq v \in \ker X$ then we have $0 \neq h(X)(v) = N(v) = X(v) = 0$, a contradiction. ♣

Corollary 2. *x has a JCD iff x is locally finite and $x|_{\mathbb{V}^p(x)}$ has a JCD for each p in the spectrum of x.*

Proof.
$\Rightarrow$ By Proposition 1(i) x is locally finite and by Proposition 1(iii) $\mathbb{V}^p(x)$ is s and hence n-invariant. It is now clear that $(s|_{\mathbb{V}^p(x)}, n|_{\mathbb{V}^p(x)})$ is a JCD of $x|_{\mathbb{V}^p(x)}$.
$\Leftarrow$ Use Theorem 1.1.1. ♣

Proposition 3. *Let $y \in End_{\mathbb{K}}(\mathbb{V})$. Then $y \in \mathbb{K}[x]$ iff $y_{\mathbb{F}} \in \mathbb{F}[x_{\mathbb{F}}]$.*

Proof. One implication is obvious. For the other, suppose by contradiction that $y \notin \mathbb{K}[x] \subset End_{\mathbb{K}}(\mathbb{V})$. Then $1 \otimes y \notin \mathbb{F} \bigotimes \mathbb{K}[x] \subset \mathbb{F} \bigotimes End_{\mathbb{K}}(\mathbb{V})$ and therefore $y_{\mathbb{F}} \notin \mathbb{F}[x_{\mathbb{F}}] \subset End_{\mathbb{F}}(\mathbb{V}_{\mathbb{F}})$. Indeed, the natural embedding $\mathbb{F} \bigotimes End_{\mathbb{K}}(\mathbb{V}) \rightarrow End_{\mathbb{F}}(\mathbb{V}_{\mathbb{F}})$ maps $\mathbb{F} \bigotimes \mathbb{K}[x]$ onto $\mathbb{F}[x_{\mathbb{F}}]$ and sends $1 \otimes y$ to $y_{\mathbb{F}}$.

Proposition 4. *Let $y \in End_{\mathbb{K}}(\mathbb{V})$ and suppose that x is algebraic. Then $y \in \mathbb{K}[x]$ if and only if*
(i) $V^p(x)$ is invariant under y for each $p \in spec(x)$.
(ii) $y|_{V^p(x)} \in \mathbb{K}[x|_{V^p(x)}]$ for each $p \in spec(x)$.

Proof.

Necessity. Clear.

Sufficiency. If $\mathbf{V} \neq (0)$ then $p_x = p_1^{k_1} \cdots p_l^{k_l}$ for some $l \in \mathbb{N}$ and $p_i \in \mathcal{P}$. Thus $spec(x) = \{p_1, \cdots, p_l\}$ is finite. If $l = 1$ there is nothing to prove. If $l > 1$ then for each $1 \leq i \leq l$ take $q_i \in \mathbb{K}[t]$ such that $q_i[x|_{V^{p_i}(x)}] = y|_{V^{p_i}(x)}$ and let $g_i = \prod_{j \neq i} p_i^{k_i}$.

Since the g_i's are coprime $1 = h_1 g_1 + \cdots + h_l g_l$ for some $h_i \in \mathbb{K}[t]$. Now let $q = q_1 h_1 g_1 + \cdots + q_l h_l g_l$. Then for each $1 \leq i \leq l$ we have:

$$q(x)|_{V^{p_i}(x)} = q_i(x)|_{V^{p_i}(x)} = q_i(x|_{V^{p_i}(x)}) = y|_{V^{p_i}(x)}.$$

We conclude from Theorem 1.1.1 that $q(x) = y$. ♣

Proposition 5. *Assume x has a Jordan-Chevalley decomposition (s, n).*

(i) This decomposition is absolute iff x is separable.

Suppose now that x is separable. Then:

(ii) (s, n) is the unique Jordan-Chevalley decomposition of x.

(iii) $(s_{\mathbb{F}}, n_{\mathbb{F}})$ is the unique Jordan-Chevalley decomposition of $x_{\mathbb{F}}$.

(iv) If $\mathbf{W}$ is any x-invariant subspace of $\mathbf{V}$ then $\mathbf{W}$ is s and n-invariant and $(s|\mathbf{W}, n|\mathbf{W})$ is the unique Jordan-Chevalley decomposition of $x|\mathbf{W}$.

(v) (s, n) is standard.

Proof.

(i) We have $CR(x) = CR(s)$ by Proposition 1. Now (i) follows from Proposition 1.5.2(v)

(ii) Note that $s_{\overline{\mathbb{K}}}$ is semisimple by (i) and that $n_{\overline{\mathbb{K}}}$ is locally nilpotent by Note 1.5.1. Since the functor "extending scalars to $\overline{\mathbb{K}}$" is faithful we can assume that $\mathbb{K}$ is algebraically closed. By Proposition 1(iii), s acts by multiplication by a in $\mathbf{V}^a(x)$, $\forall a \in \mathbb{K}$. Since $\mathbf{V} = \bigoplus_{a \in \mathbb{K}} \mathbf{V}^a(x)$, s, and hence n, are completely determined.

(iii) We only have to prove uniqueness. Due to (i) and (ii) it suffices to show that $s_{\mathbb{F}}$ absolutely semisimple. Use Note 1.3.2 for this purpose.

(iv) It is enough to demonstrate that $\mathbf{W}$ is s (or n)-invariant. Since this happens iff $\mathbf{W}_{\overline{\mathbb{K}}}$ is $s_{\overline{\mathbb{K}}}$ (or $n_{\overline{\mathbb{K}}}$)-invariant, we can assume again that $\mathbb{K}$ is algebraically closed.

In this case $\mathbb{W} = \bigoplus_{a \in \mathbb{K}} \mathbb{W} \cap \mathbb{V}^a(x) = \bigoplus_{a \in \mathbb{K}} \mathbb{W} \cap \mathbb{V}_a(s)$ is s-invariant, for s acts like a scalar in each $\mathbb{W} \cap \mathbb{V}_a(s)$.

(v) Pick any x-invariant subspace $\mathbb{U}$ of $\mathbb{V}$. We have to prove that if $X = x|_{\mathbb{U}}$ is algebraic then $S = s|_{\mathbb{U}}, N = n|_{\mathbb{U}} \in \mathbb{K}[X]$. Due to Note 1.5.1, (iii) and Proposition 3 (in this order) we can suppose once more that $\mathbb{K}$ is algebraically closed. Since S and N act like a and $X - a$ in $\mathbb{U}^a(X)$ respectively for each $a \in spec(\mathbb{U}(X)) \subset \mathbb{K}$ we apply Proposition 4 (to $y = S$) to obtain the desired result. ♣

Theorem 1. *Let $\mathbb{K}$ be a field, $\mathbb{V}$ a vector space over $\mathbb{K}$ and $x \in End_{\mathbb{K}}(\mathbb{V})$. Then x has an absolute Jordan-Chevalley decomposition (s, n) iff*

(i) x is locally finite.

(ii) x is separable.

Moreover if (i) and (ii) hold then (s, n) is standard and it is the unique Jordan-Chevalley decomposition that x has.

The above decomposition will be sometimes denoted (x_s, x_n).

Proof.

Existence-Necessity. x is separable by Proposition 5(i) and locally finite by Proposition 1(i).

Existence-Sufficiency. We divide the proof into 3 stages.

Stage 1. x is algebraic and $E(x) \subset \mathbb{K}$.

If $p_x = (t - a_1)^{r_1} \cdots (t - a_k)^{r_k}$, define s and n to act like a_i and $x - a_i$ in $\mathbb{V}^{a_i}(x)$.

Stage 2. x is algebraic and separable.

Let $\mathbb{F}$ be the splitting of p_x over $\mathbb{K}$. Then $\mathbb{F}/\mathbb{K}$ is a Galois extension. Let (S, N) be the JCD of $x_{\mathbb{F}}$. As shown in the first stage, S is diagonalizable.

Let $M_I(\mathbb{F})$ be the $\mathbb{F}$-algebra of all matrices $M\colon I \times I \to \mathbb{F}$ of almost zero columns. Fix a basis $(v_i)_{i \in I}$ of $\mathbb{V}$ over $\mathbb{K}$ and let $A \in M_I(\mathbb{K})$ and B, $C \in M_I(\mathbb{F})$ be the respective matrices of $x_{\mathbb{F}}, S$ and N with respect to $(1 \otimes v_i)_{i \in I}$. We want to show that B, $C \in M_I(\mathbb{K})$ as well. To see this pick any $\sigma \in Gal(\mathbb{F}/\mathbb{K})$.

We can extend σ to an $\mathbb{K}$-algebra automorphism $\tilde{\sigma}$ of $M_I(\mathbb{F})$ fixing $M_I(\mathbb{K})$ defined by $M \mapsto M^{\sigma} = \sigma \circ M$.

If S_σ and N_σ are the $\mathbb{F}$-endomorphisms of $\mathbb{V}_\mathbb{F}$ whose matrices with respect to $(1 \otimes v_i)_{i \in I}$ are B^σ and C^σ, then (S_σ, N_σ) is the JCD of $x_\mathbb{F}$. Indeed:

(i) $A = A^\sigma = B^\sigma + C^\sigma$, so $x_\mathbb{F} = S_\sigma + N_\sigma$.

(ii) $B^\sigma C^\sigma = (BC)^\sigma = (CB)^\sigma = C^\sigma B^\sigma$, so $[S_\sigma, N_\sigma] = 0$.

(iii) Since S is diagonalizable B is similar to a diagonal matrix and hence so must be B^σ. Thus S_σ is diagonalizable.

(iv) Note that each $(1 \otimes v_i)$ is killed by some power of N_σ. Hence N_σ is locally nilpotent.

By uniqueness (Proposition 5(ii)) $S = S_\sigma$ and $N = N_\sigma$, so that $B^\sigma = B$ and $C^\sigma = C$. Since this holds for every $\sigma \in Gal(\mathbb{F}/\mathbb{K})$ we obtain the desired relation: $B, C \in M_I(\mathbb{K})$ (see Stewart [89], chapter 10). This shows that $S = s_\mathbb{F}$ and $N = n_\mathbb{F}$ for unique $s, n \in End_\mathbb{K}(\mathbb{V})$, thus obtaining the JCD $(s, n) = (x_s, x_n)$ of x.

Stage 3. General case.

We have no choice but to define $s(v) = (x|Z(x,v))_s(v)$ and $n(v) = (x|Z(x,v))_n(v)$ $\forall v \in \mathbf{V}$.

Using Proposition 5(iv) we verify that $s|\mathbb{W} = (x|\mathbb{W})_s$ and $n|\mathbb{W} = (x|\mathbb{W})_n$ for each finite dimensional x-invariant subspace $\mathbb{W}$ of $\mathbb{V}$, which readily shows that s and n are semisimple and locally nilpotent endomorphisms of $\mathbb{V}$, respectively. Moreover, $x = s + n$ and $[s, n] = 0$ because this happens in each finite dimensional x-invariant subspace of $\mathbb{V}$ and their sum is $\mathbb{V}$. Hence (s, n) is the JCD of x.

The remaining assertions were proved in Proposition 5. ♣

We now turn to study the existence of standard JCD.

Proposition 6.

(i) If x is semisimple then $q(x)$ locally nilpotent implies $q(x) = 0$ for any $q(t) \in \mathbb{K}[t]$. The converse is false, even if x is locally finite. It is true, however, if x is algebraic and therefore x is semisimple and algebraic iff $\mathbb{K}[x]$ is semisimple.

(ii) If x is semisimple then every element of $\mathbb{K}[x]$ is semisimple.

Proof.

(i) Pick any $q(t) \in \mathbb{K}[t]$ such that $q(x)$ is locally nilpotent and any $0 \neq v \in \mathbf{V}$. Then $q^k(x)(v) = 0$ for some $k \in \boldsymbol{N}$. Thus $p_{x,v}|q^k$. Since x is semisimple $p_{x,v}$ is a product of distinct primes. This gives $p_{x,v}|q$ and therefore $q(x)(v) = 0$.

For the counterexample, construct x such that $\mathbf{V}(x) = \bigoplus_{p\in\mathcal{P}} \mathbf{V}^p(x)$ with $\mathbf{V}^p(x) \neq \mathbf{V}_p(x)$ for all $p \in \mathcal{P}$ (which is perfectly possible). Note that $\mathcal{P}$ is infinite (Euclid). If $q = p_1^{r_1} \cdots p_k^{r_k}$ for some $p_i \in \mathcal{P}$ and $r_i \in \boldsymbol{N}$, then pick $p \in \mathcal{P} \setminus \{p_1, \cdots, p_k\}$ and observe that $q(x)$ is an automorphism of $\mathbf{V}^p(x)$, by Proposition 1.1.3, and then so is $q^k(x)$ $\forall k \in \boldsymbol{N}$. Thus no non-zero polynomial in x is locally nilpotent but x is locally finite and not semisimple.

But if x is algebraic and not semisimple then $p_x = p_1^{r_1} \cdots p_k^{r_k}$ with some $r_i > 1$, so $p_1 \cdots p_k(x)$ is non-zero nilpotent. The last assertion is now clear.
(ii) Let $q \in \mathbb{K}[t]$. If $\mathbb{W}$ is a finite dimensional x-invariant subspace of $\mathbf{V}$ then $\mathbb{W}$ is $q(x)$-invariant and $q(x)|\mathbb{W} = q(x|\mathbb{W})$. A correct application of (i) yields that $q(x)|\mathbb{W}$ is semisimple. It readily follows that $q(x)$ is semisimple. ♣

Theorem 2. *Let $\mathbb{K}$ be a field, $\mathbf{V}$ a vector space over $\mathbb{K}$ and $x \in End_{\mathbb{K}}(\mathbf{V})$.*
Then x has a standard Jordan-Chevalley decomposition if and only if
(i) x is locally finite.
(ii) For all $p \in \mathcal{P}$, if p is not separable over $\mathbb{K}$ then $\mathbf{V}_p(x) = \mathbf{V}^p(x)$.
Moreover if (i) and (ii) hold then x has a unique standard Jordan-Chevalley decomposition.

Proof.

Existence-Sufficiency. Construct a Jordan-Chevalley decomposition (s, n) of x as follows:

Pick any $p \in spec(x)$. If p is separable over $\mathbb{K}$ then declare $s|_{V^p(x)}$ and $n|_{V^p(x)}$ to be the semisimple and nilpotent parts of $x|_{V^p(x)}$ (see Theorem 1). If p is not separable over $\mathbb{K}$ then x acts semisimply on $V^p(x)$ by hypothesis, so we set $s|_{V^p(x)} = x|_{V^p(x)}$ and $n|_{V^p(x)} = 0$. Since x is locally finite $\mathbf{V} = \bigoplus V^p(x)$ (see Proposition 1.2.1) and s and n are well-defined endomorphisms of $\mathbf{V}$. It is clear that (s, n) is a Jordan-Chevalley decomposition of x.

To see that (s,n) is a standard JCD of x pick any x-invariant subspace $\mathbb{U}$ of $\mathbb{V}$. Let $\mathcal{P}_1 = \{p \in spec(x) | p \text{ is separable over } \mathbb{K}\}$ and $\mathbb{U}_1 = \bigoplus_{p\in\mathcal{P}_1}(\mathbb{U} \cap V^p(x))$. $\mathbb{U}_1$ is s and n-invariant by Proposition 5(iv). Now let $\mathcal{P}_2 = spec(x) \setminus \mathcal{P}_1$ and $\mathbb{U}_2 = \bigoplus_{p\in\mathcal{P}_2}(\mathbb{U} \cap V^p(x))$. $\mathbb{U}_2$ is invariant under s and n by definition. Since $\mathbb{U} = \mathbb{U}_1 \bigoplus \mathbb{U}_2$ by Proposition 1.1.1(ii) $\mathbb{U}$ is then invariant under s and n.

Now suppose that $x|_{\mathbb{U}}$ is algebraic. Then $s|_{\mathbb{U}_1}$ and $n|_{\mathbb{U}_1}$ are in $\mathbb{K}[x|_{\mathbb{U}_1}]$ by Theorem 1 and $s|_{\mathbb{U}_2}$ and $n|_{\mathbb{U}_2}$ are in $\mathbb{K}[x|_{\mathbb{U}_2}]$ by definition. Hence $s|_{\mathbb{U}}$ and $n|_{\mathbb{U}}$ are in $\mathbb{K}[x|_{\mathbb{U}}]$ by Proposition 4.

Existence-Necessity. We only need to show that (ii) is necessary. Suppose that $p \in spec(x)$ is not separable over $\mathbb{K}$. *We claim that x acts semisimply on $\mathbb{V}^p(x)$.* If not, pick $v \in \mathbb{V}^p(x)$ such that $p_{x,v} = p^k$ for some $k > 1$ and let $\mathbb{U} = Z(x,v)$. Then $\mathbb{U}$ is finite dimensional and its minimal polynomial is p^k.

Let $X = x|_{\mathbb{U}}$, $S = s|_{\mathbb{U}}$ and $N = n|_{\mathbb{U}}$. By hypothesis $S, N \in \mathbb{K}[X]$. Note that the Jacobson radical J of $\mathbb{K}[X]$ is $(p(X))$ and contains N, and therefore we must have $S = X + p(X)q(X)$ for some $q \in \mathbb{K}[t]$ (2).

Since p is not separable over $\mathbb{K}$, $p = a_o + a_1 t^q + \cdots + a_m t^{mq}$ for some $a_i \in \mathbb{K}$, where $0 < q = char\mathbb{K}$.

By Proposition 1(iii) we have $p(S) = 0$. Using (2) we obtain

$$\begin{aligned} a_o &= a_o \\ a_1 S^q &= a_1 X^q + p(X)^q g_1(X) \\ &\vdots \qquad\qquad \vdots \\ a_m S^{mq} &= a_1 X^{mq} + p(X)^q g_m(X) \end{aligned} \tag{3}$$

for some $g_1, \cdots, g_m \in \mathbb{K}[t]$. Summing up (3) we obtain:
$0 = p(S) = p(X) + p(X)^q h(X) = p(X)(1 + p(X)^{q-1} h(X))$ for some $h \in \mathbb{K}[t]$. But $(1 + p(X)^{q-1} h(X))$ is a unit in $\mathbb{K}[X]$. Hence $p(X) = 0$, contradicting $\mathbb{V}^p(x) \neq \mathbb{V}_p(x)$.

Uniqueness. Suppose that (s', n') is a standard JCD of x different from (s,n). Then s and s' differ in some primary component $\mathbb{V}^p(x)$ and moreover by Theorem

1 we may assume that p is not separable over $\mathbb{K}$. Pick $v \in \mathbb{V}^p(x)$ such that $s(v) \neq s'(v)$ and let $\mathbb{U} = Z(x, v)$. Then $s'|_{\mathbb{U}} \in \mathbb{K}[x|_{\mathbb{U}}] = \mathbb{K}[s|_{\mathbb{U}}]$ by definition of s. Thus $n'|_{\mathbb{U}} = s|_{\mathbb{U}} - s'|_{\mathbb{U}}$ is nilpotent, and hence $s|_{\mathbb{U}} - s'|_{\mathbb{U}} = 0$ by Proposition 6(i), a contradiction. ♣

Corollary 3. *If x algebraic and satisfies (ii) in Theorem 1.3.2 then:*
(i) There is a unique JCD (s, n) of x with $s, n \in \mathbb{K}[x]$.
(ii) s and n are algebraic and their minimal polynomials are the product of the primes in $\mathcal{P}$ dividing p_x and t^k, respectively, where k is the largest of the exponents to which those primes are raised in the (monic) decomposition of p_x.

Proof.

(i) See Theorem 2.

(ii) The whole statement about s follows from Proposition 1(iii) and Proposition 1.2.1(ii). Take any $p \in spec(x)$. If p is not separable then $n|\mathbb{V}_p(x) = 0$. If p is separable and $x|\mathbb{V}^p(x)$ has minimal polynomial p^l then extend scalars to see that $n|\mathbb{V}^p(x)$ is algebraic with minimal polynomial equal to t^l. The result follows. ♣

Corollary 4. *Suppose that x is cyclic. The following conditions are equivalent:*
(i) x has a unique Jordan-Chevalley decomposition.
(ii) x has a Jordan-Chevalley decomposition.
(iii) x is locally finite and $\mathbb{V}^p(x) \neq \mathbb{V}_p(x)$ implies p separable over $\mathbb{K}$ for any $p \in \mathcal{P}$.

Proof.

(i)⇒(ii) Clear.

(ii)⇒(iii) If x is cyclic then any endomorphism commuting with x belongs to $\mathbb{K}[x]$ (see Proposition 7 below). Thus any JCD of x is standard and we can apply Theorem 2 to obtain (iii).

(iii)⇒(i) See Theorem 2. ♣

For the sake of completeness we provide several conditions equivalent to an endomorphism being cyclic.

Proposition 7. *Assume $dim_{\mathbb{K}}(\mathbb{V}) = n \in \mathbb{N}$. Let A be any matrix in $M_n(\mathbb{K})$*

representing x. The following conditions are equivalent:

(i) x is cyclic.

(ii) The minimal polynomial of x has degree n.

(iii) The characteristic and minimal polynomials of x coincide.

(iv) x acts cyclicly on any invariant subspace of $\mathbb{V}$.

(v) The Jordan form of $x_{\overline{\mathbb{K}}}$ has only one cell per eigenvalue.

(vi) The rational form of x has only one invariant factor.

(vii) The $(n-1)$-minors of $t1_n - A \in M_n(\mathbb{K}[t])$ are coprime.

(viii) The commutator of x is commutative.

(ix) The commutator of x is $\mathbb{K}[x]$.

(x) The commutator of x has dimension n.

(xi) $x_{\mathbb{F}}$ is cyclic for every field extension $\mathbb{F}$ of $\mathbb{K}$.

Proof. We only show the implication that we need, namely (i)⇒(ix). The rest is left to the reader. Since this result is required in Corollary 4 the forthcoming argument will not make use of the assumption that $\mathbb{V}$ is finite dimensional.

Take any $y \in End_{\mathbb{K}}(\mathbb{V})$ commuting with x and let $v \in \mathbb{V}$ be an x-generator of $\mathbb{V}$. Then $y(v) = p(x)(v)$ for some $p \in \mathbb{K}[t]$. Given $w \in \mathbb{V}$ we have $w = q(x)(v)$ for some $q \in \mathbb{K}[t]$ and $y(w) = q(x)p(x)v = p(x)q(x)v = p(x)w$, so that $y = p(x) \in \mathbb{K}[x]$.♣

Remark. We will see in Example 3 that an endomorphism may have different Jordan-Chevalley decompositions. Example 6 shows an endomorphism with no JCD whatsoever. However we do not provide necessary and sufficient conditions for an endomorphism x to have a JCD or a criterion to decide when this decomposition is unique.

In view of Corollary 2 and Theorem 1 these problems can be reduced to the case $\mathbf{V} = \mathbf{V}^p(x)$ where p is not separable over the ground field $\mathbb{K}$. Corollary 4 is the only partial answer we can give in this case. However, we conjecture that x will have a JCD if and only if $\mathbb{V}^p(x) = \mathbb{V}_p(x)$. We close this section with a rather short proof of the following:

Proposition 8. *If x satisfies (i) and (ii) of Theorem 2 and $y \in End_{\mathbb{K}}(\mathbf{V})$ com-*

mutes with x then y commutes the semisimple and nilpotent parts of the standard Jordan-Chevalley decomposition of x.

Proof. Since this holds trivially in the primary components corresponding to non-separable polynomials (if they exist at all), we can assume that $\mathbb{K}$ is algebraically closed. From $[y,x]=0$ we conclude that $\mathbb{V}^a(x)$ is y-stable for each $a \in \mathbb{K}$. Since the semisimple part of x is a scalar there, the result follows. ♣

1.7. Triangularizable endomorphisms

We show that a finite family of commuting locally finite triangularizable endomorphisms can be simultaneously triangularized. Since this type of endomorphisms can be characterized as those whose semisimple part is diagonalizable we preferred to present this material after the JCD's were introduced.

Proposition 1. *The following conditions are equivalent:*
(i) x has a Jordan-Chevalley decomposition (s,n) with s diagonalizable.
(ii) x is split (i.e.$\mathbb{V}=\bigoplus_{a\in\mathbb{K}}\mathbb{V}^a(x)$).
(iii) x is triangularizable and locally finite.
(iv) x is locally finite and $E(x)\subset\mathbb{K}$.

Proof.
(i)⇒(ii). $E(x)=E(s)\subset\mathbb{K}$ and x is locally finite, by Proposition 1.6.1 and Proposition 1.5.1. Thus every p in the spectrum of x is linear and x is split.
(ii)⇒(iii). We need to see that x is triangularizable. We can restrict ourselves to $\mathbb{V}=\mathbb{V}^a(x)$ $a\in\mathbb{K}$, and indeed to $\mathbb{V}=\mathbb{V}^o(x)$, because once this is proved, if $\mathbb{V}=\mathbb{V}^a(x)$ then $\mathbb{V}=\mathbb{V}^o(x-a)$ and the totally ordered basis B that triangularizes $x-a$ also triangularizes $x=(x-a)+a$. Thus we can assume that x is locally nilpotent.

Let $\mathcal{A}$ be the collection of all pairs $(B,\leq)$ such that B is an independent system of vectors of $\mathbb{V}$, $\leq$ is a total order on B, the subspace $\mathbb{K}B$ generated by B is invariant under x and $x|_{\mathbb{K}B}$ is triangularized by B. Order $\mathcal{A}$ by inclusion, namely $(B,\leq)$ precedes $(B',\leq')$ if $B\subset B'$ and $\leq\subset\leq'$. $\mathcal{A}$ is non-empty for 0 is an eigenvalue

of x. Zorn's Lemma can be applied to obtain a maximal member $(B, \leq)$ of $\mathcal{A}$. If $\mathbb{K}B \neq \mathbb{V}$ pick any $v \in \mathbb{V} \setminus \mathbb{K}B$. The x-conductor p of v in $\mathbb{K}B$ divides $p_{x,v}$ and hence $p = t^k$ for some $k \geq 1$. Let $B' = B \cup \{x^{k-1}(v), \cdots, v\}$. The definition of x-conductor guarantees that B' is linearly independent. Ordering B' correctly, say by $\leq'$, we see that $(B', \leq')$ is in $\mathcal{A}$ and strictly follows $(B, \leq)$, a contradiction.
(iii)⇒(iv). Let $\lambda \in E(x) \subset \overline{\mathbb{K}}$ and $u \in \mathbb{V}_{\overline{\mathbb{K}}}$ be an eigenvector corresponding to λ. Let B be a totally ordered basis triangularizing x. There are unique $k \in \boldsymbol{N}$, $(v_i)_{1 \leq i \leq k} \in B$ and $(\alpha_i)_{1 \leq i \leq k} \in \overline{\mathbb{K}}$ such that $v_1 < v_2 < \cdots < v_k$ $\alpha_i \neq 0$ and $u = \sum_{i=1}^{k} \alpha_i \otimes v_i$. The $1 \otimes v_k$-coordinate of λu is $\lambda \alpha_k$. By the way $x_{\overline{\mathbb{K}}}$ operates and x being triangularizable that coordinate is also $a\alpha_k$ for some $a \in \mathbb{K}$. Since $\alpha_k \neq 0$, we have $\lambda = a \in \mathbb{K}$.
(iv)⇒(i). Use Theorem 1.6.1 and then Propositions 1.6.1 and 1.5.1. ♣

Corollary 1. *If x is locally finite and triangularizable then x is locally finite and triangularizable in any x-invariant subspace of $\mathbb{V}$.*

Proposition 2. *Let $x_1, \cdots, x_n$ be commuting endomorphisms of $\mathbb{V}$. Then:*
(i) If the x_i's are diagonalizable there is basis of $\mathbb{V}$ which simultaneously diagonalizes them all and, hence, every endomorphism in $\mathbb{K}[x_1, \cdots, x_n]$.
(ii) (i) holds if we replace diagonalizable by locally finite triangularizable.
(iii) If the x_i's are absolutely semisimple then every endomorphism in $\mathbb{K}[x_1, \cdots, x_n]$ is absolutely semisimple.
(iv) (iii) holds if we replace absolutely semisimple by any of the following: locally finite, algebraic and locally nilpotent.

Proof.
(i) By induction on n. The case $n = 1$ being trivial, assume the result holds for some $n \in \boldsymbol{N}$.

Given commuting diagonalizable endomorphisms $x_1, \cdots, x_n, x_{n+1}$, every x_i stabilises and acts diagonally in each $\mathbb{V}_a(x_1)$ for all $a \in \mathbb{K}$ (see Proposition 1.1.1(ii)). Now apply the inductive hypothesis to obtain the desired basis.
(ii) We need the following:

Lemma. *Under the same hypothesis of (ii), if* $\mathbf{W} \subset \mathbf{V}$ *is a proper subspace of* $\mathbf{V}$ *invariant under the* $x_i's$*, then there are* $v \in \mathbf{V} \setminus \mathbf{W}$ *and* $(\alpha_i)_{1 \leq i \leq n}$ *in* $\mathbb{K}$ *such that* $\alpha_i \in CR(x_i)$ *and* $(x_i - \alpha_i)(v) \in \mathbf{W}$.

Proof. By induction on n. If $n = 1$ and $\mathbf{W}$ is x-invariant and proper, let $w \in \mathbf{V} \setminus \mathbf{W}$. By Proposition 3 $x = x_1$ is locally finite and $CR(x) \subset \mathbb{K}$. Thus, $p_{x,w}$ is a product of linear factors and so must then be the x-conductor of w in $\mathbf{W}$ which divides it. If $p = (t - a_1) \cdots (t - a_n)$ is the x-conductor of w in $\mathbf{W}$ then the x-conductor of $v = (x - a_1) \cdots (x - a_{n-1})$ in $\mathbf{W}$ is $t - a_n$, so $v \in \mathbf{V} \setminus \mathbf{W}$ and $(x - a_n)(v) \in \mathbf{W}$.

Now assume the Lemma holds for some $n \in \mathbb{N}$ and that $\mathbf{W}$ is x-invariant under $x_1, \cdots, x_n, x_{n+1}$ and proper. By the case $n = 1$ $\mathbf{W}$ is properly contained in $\mathbf{V}_1 = \{v \in \mathbf{V} | (x_1 - a)(v) \in \mathbf{W}\}$, for some $a \in CR(x_1)$. Since $\mathbf{W}$ is invariant under the x_i's and they commute, $\mathbf{V}_1$ is also invariant under $x_2, \cdots, x_{n+1}$ and by Corollary 1 they are locally finite, triangularizable and commute on $\mathbf{V}_1$. We now apply the inductive hypothesis to finish.

Proof of (ii). Let $\mathcal{A}$ be the collection of all pairs $(B, \leq)$ such that B is an independent system of vectors of $\mathbf{V}$, $\leq$ is a total order on B, the subspace $\mathbb{K}B$ generated by B is invariant for all x_i and $x_i|_{\mathbb{K}B}$ is triangularized by B for all i. Order $\mathcal{A}$ by inclusion, namely $(B, \leq)$ precedes $(B', \leq')$ if $B \subset B'$ and $\leq \subset \leq'$. Apply the Lemma to $\mathbf{W} = (0)$ obtaining a common eigenvector. Thus $\mathcal{A}$ is non-empty. Check that Zorn's Lemma can be applied and obtain a maximal member $(B, \leq)$ of $\mathcal{A}$. If $\mathbb{K}B \neq \mathbf{V}$ apply the Lemma to obtain a member of $\mathcal{A}$ greater than $(B, \leq)$,a contradiction. Hence B simultaneously triangularizes the $x_i's$, and consequently every endomorphism in $\mathbb{K}[x_i \cdots, x_n]$.

(iii) Let $\mathbb{F} = \overline{\mathbb{K}}$. Then $(x_1)_{\mathbb{F}}, \cdots, (x_n)_{\mathbb{F}}$ are in the conditions of (i), so every element of $\mathbb{F}[(x_1)_{\mathbb{F}}, \cdots, (x_n)_{\mathbb{F}}]$ and hence of $\mathbb{K}[(x_1)_{\mathbb{F}}, \cdots, (x_n)_{\mathbb{F}}]$ is diagonalizable. If $y \in \mathbb{K}[x_1, \cdots, x_n]$ then $y_{\mathbb{F}} \in \mathbb{K}[(x_1)_{\mathbb{F}}, \cdots, (x_n)_{\mathbb{F}}]$ (the functor "extension of scalars to $\mathbb{F}$" is $\mathbb{K}$-linear). Thus, y is absolutely semisimple by Proposition 1.5.2.

(iv) The locally finite and locally nilpotent cases were proved in Proposition 1.6.1. Note finally that algebraic means integral over $\mathbb{K}$. ♣

Example 3 shows that (iii) is false for semisimple endomorphisms.

1.8. Applications. Classically separable algebras

We now explore the connection between Jordan-Chevalley decompositions and the Wedderburn-Malcev Theorem for finite dimensional associative, commutative and unital algebras over a field; in this context the Theorem involves the concept of classically separable algebras. Separable algebras are treated in chapter 2 and a general version of the Theorem is proved in chapter 3.

Definition 1. An associative unital algebra A over $\mathbb{K}$ is **classically separable** if for any field extension $\mathbb{F}$ of $\mathbb{K}$, $J(\mathbb{F} \bigotimes A) = (0)$.

The following characterization of finite dimensional commutative classically separable algebras is proven using the material developed in the previous sections. A better result is given in the chapter 2.

Proposition 1. *Let A be a finite dimensional associative, commutative and unital algebra over $\mathbb{K}$. Then A is classically separable iff the minimal polynomial (over $\mathbb{K}$) of every non-zero element of A is a product of distinct separable primes over $\mathbb{K}$. In particular, classically separable and separable mean the same for finite dimensional field extensions.*

Proof We can assume $A = \mathbb{K}[x_1 \cdots x_n]$, where $0 \neq x_i \in End_{\mathbb{K}}(\mathbf{V})$ for some *f.d.* $\mathbb{K}$-space $\mathbf{V}$ (using the left regular representation of A). Now, A is classically separable iff $\mathbb{K}[x_1 \cdots x_n] \bigotimes_{\mathbb{K}} \mathbb{F} \simeq \mathbb{F}[(x_1)_{\mathbb{F}}, \cdots, (x_n)_{\mathbb{F}}]$ is semisimple for every field extension $\mathbb{F}$ of $\mathbb{K}$ iff $((x_i)_{\mathbb{F}})_{\leq i \leq n}$ is a semisimple endomorphism for every field extension $\mathbb{F}$ of $\mathbb{K}$ iff x_i is an absolutely semisimple endomorphism $\forall i : 1 \leq i \leq n$ iff the minimal polynomial of x_i (over $\mathbb{K}$) is a product of distinct separable primes over $\mathbb{K}$.

Since the x_i are arbitrary generators of A, the property is proven. ♣

The next result gives necessary and sufficient conditions for the following particular instance of Wedderburn-Malcev Theorem to hold.

Proposition 2. *The following conditions are equivalent:*

(i) x is algebraic and $\mathbf{V}^p(x) \neq \mathbf{V}_p(x)$ implies p separable over $\mathbb{K}$ for any $p \in \mathcal{P}$.

(ii) There is a subalgebra A of $\mathbb{K}[x]$ such that:

(a) A is semisimple.

(b) $\mathbb{K}[x] = A \bigoplus J(\mathbb{K}[x])$.

Moreover the subalgebra A of (ii) is unique.

Proof.

(i) $\Rightarrow$ (ii). Let (s, n) is the standard Jordan-Chevalley decomposition of x (see Theorem 1.6.2) and set $A = \mathbb{K}[s]$. A is semisimple by Proposition 1.6.6(i) while the fact that $\mathbb{K}[x] = \mathbb{K}[s] + \mathbb{K}[x]n$ is immediate. Moreover $\mathbb{K}[x]n \subset J(\mathbb{K}[x])$ and $J(\mathbb{K}[x]) \cap \mathbb{K}[s] = \mathbb{K}[x]n \cap \mathbb{K}[s] = (0)$ since $\mathbb{K}[s]$ contains no non-zero nilpotent element. Hence $J(\mathbb{K}[x]) = \mathbb{K}[x]n$ and $\mathbb{K}[x] = A \bigoplus J(\mathbb{K}[x])$.

(ii) $\Rightarrow$ (i). First note that x is algebraic. If not $\mathbb{K}[t] \simeq \mathbb{K}[x]$ and hence $\mathbb{K}[x]$ is not semisimple and $J(\mathbb{K}[x]) = (0)$, contradicting (ii). Every element of A is algebraic by Proposition 1.7.2(iv) and A does not contain non-zero nilpotent elements. Hence every endomorphism in A is semisimple by Proposition 1.6.6(i). Now using (b) we obtain the standard Jordan-Chevalley decomposition (s, n) of x. Thus (i) follows from Theorem 1.6.2.

Moreover since $\mathbb{K}[s] \subset A$ and, as shown in (i), $\mathbb{K}[x] = \mathbb{K}[s] \bigoplus J(\mathbb{K}[x])$ we conclude that $A = \mathbb{K}[s]$ is unique. ♣

If we require x above to be separable we can improve the previous result. Indeed, we give necessary and sufficient conditions for the Wedderburn-Malcev Theorem to hold in the more general setting of finite dimensional associative, commutative and unital algebras over a field. More precisely we have:

Proposition 3. *Let A be a finite dimensional (unital and associative) commutative algebra over $\mathbb{K}$. The following conditions are equivalent:*

(i) There is a classically separable subalgebra S of A such that $A = S \bigoplus J(A)$.

(ii) The minimal polynomial of every non-zero element of A is separable over $\mathbb{K}$.

Moreover, the subalgebra S is unique.

Proof. Using the left regular representation of A we can assume $A = \mathbb{K}[x_1, \cdots, x_n]$, where the x_i's are commuting endomorphisms of some finite dimensional $\mathbb{K}$-space.
(ii)⇒(i) Let (s_i, n_i) be the absolute Jordan-Chevalley decomposition of x_i, for each $1 \leq i \leq n$. Set $S = \mathbb{K}[s_1, \cdots, s_k]$. Then S is a finite dimensional commutative algebra due to Proposition 1.6.8. Note also that the n_i's are nilpotent.

S is classically separable (and hence semisimple) as the proof of Proposition 1 shows. Therefore $S \cap A\mathbb{K}[n_1, \cdots, n_k] = S \cap J(A) = (0)$. For any $(r_i)_{1 \leq i \leq k}$ we have $x_1^{r_1} \cdots x_1^{r_k} = (s_1 + n_1)^{r_1} \cdots (s_k + n_k)^{r_k} = s_1^{r_1} \cdots s_k^{r_k} + y$, where $y \in A\mathbb{K}[n_1, \cdots, n_k]$. It follows that $A = S \bigoplus A\mathbb{K}[n_1, \cdots, n_k]$. Hence $J(A) = A\mathbb{K}[n_1, \cdots, n_k]$ and $A = S \bigoplus J(A)$.
(i)⇒(ii) Pick any $0 \neq x \in A$ then $x = s + n$ for unique $s \in S$ and $n \in J(A)$. If $x = n$ then x is nilpotent and there is nothing to prove. If $x \neq n$ then $0 \neq s$ is absolutely semisimple for S is classically separable (see Proposition 1). But every prime in $\mathbb{K}[t]$ dividing p_x also divides p_s by Proposition 1.6.1(iii). Therefore p_x is separable over $\mathbb{K}$ by Proposition 1.5.3(iv).

The uniqueness statement is proved mutatis mutandis as in Proposition 2. ♣

1.9. Examples

Example 1. Let p monic irreducible in $\mathbb{K}[t] = D$. We want to construct $(\mathbf{V}, x)$ such that $\mathbf{V}(x)$ is $D(p^\infty)$, the divisible p-primary module whose socle is 1 dimensional over D/Dp (see Fuchs [70], chapter IV).

Say $p = a_o + a_1 t + \cdots + a_{n-1}t^{n-1} + t^n$. Let $\mathbb{V}$ be a $\mathbb{K}$-space with basis $(e_i)_{i\in\mathbf{N}}$. Let $A, N \in M_n(\mathbb{K})$ be defined:

$$A = \begin{pmatrix} -a_{n-1} & 1 & \dots & 0 & 0 \\ -a_{n-2} & 0 & & \vdots & \vdots \\ \vdots & \vdots & & 0 & 1 \\ -a_o & 0 & \dots & 0 & 0 \end{pmatrix} \qquad N = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 \\ \vdots & & & \vdots & \vdots \\ 0 & & & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix}$$

and x the endomorphism of $\mathbb{V}$ whose matrix in the basis $(e_i)_{i\in\mathbf{N}}$ is

$$M = \begin{pmatrix} A & N & & \\ & A & N & \\ & & A & N \\ & & & \ddots \end{pmatrix}$$. We now use the following simple:

Note (see Hungerford [74], Exercise I.3.7).

Let D be a PID p a prime in D. Then a D-module M generated by elements $x_1, x_2, x_3, \cdots$ satisfying:

(i) $px_1 = 0$ and $x_1 \neq 0$.

(ii) $px_2 = x_1$, $px_3 = x_2$, $px_4 = x_3, \cdots$.

is isomorphic to $D(p^\infty)$ via the unique isomorphism $x_i \leftrightarrow 1/p^i$, $i \in \mathbf{N}$.

Since $e_n, e_{2n}, e_{3n}, \cdots$ satisfy the above conditions, we see that $\mathbf{V}(x) \simeq D(p^\infty)$. Taking $p = t - a$, $a \in \mathbb{K}$, the Jordan-Chevalley decomposition of x is $(a, x - a)$.

Example 2. Let $\mathbb{K} = \mathbf{R}$, $\mathbf{V} = \mathbf{R}^4$ and $x \in End_{\mathbf{R}}(\mathbf{R}^4)$ be the endomorphism whose matrix in the canonical basis of $\mathbf{R}^4$ is

$$A = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

x is cyclic with minimal polynomial $p = t^4 + 2t^2 + 1 = (x^2 + 1)^2$ and has a unique Jordan-Chevalley decomposition (s, n) in $\mathbf{R}[x]$, which is four dimensional over $\mathbf{R}$

with basis $1, x, x^2+1, (x^2+1)x$, where $(x^2+1) = J(\mathbb{R}[x])$ and $s^2+1=0$. Hence $s = a_0 + a_1 x + a_2(x^2+1) + a_3(x^2+1)x$ for unique $a_i \in \mathbb{R}$ and

$$-1 = s^2 = a_0^2 - a_1^2 + 2a_0a_1x + (2a_0a_2 - 2a_1a_3 + a_1^2)(x^2+1) + 2(a_0a_3 + a_1a_2)(x^2+1)x,$$

so

$$\begin{array}{ll} (1) & -1 = a_0^2 - a_1^2 \\ (2) & 0 = 2a_0a_1 \\ (3) & 0 = 2a_0a_2 - 2a_1a_3 + a_1^2 \\ (4) & 0 = 2(a_0a_3 + a_1a_2)(x^2+1) \end{array}$$

From this and $n^2 = 0$ we conclude that $a_0 = 0$, $a_2 = 0$, $a_1 = 1$ and $a_3 = 1/2$, so that $s = x + 1/2(x^2+1)x$ and $n = -1/2(x^2+1)x$.

Example 3. (Bourbaki) Let $\mathbb{K}$ be an imperfect field of characteristic p, let a be an element of $\mathbb{K} - \mathbb{K}^p$, and let $\mathbb{L}$ be the field $\mathbb{K}(a^{1/p})$. Consider the $\mathbb{K}$-vector space $\mathbb{E} = \mathbb{L} \bigotimes_{\mathbb{K}} \mathbb{L}$; let u (resp. u') be the $\mathbb{K}$-endomorphism of $\mathbb{E}$ given by multiplication by $a^{1/p} \otimes 1$ (resp. $1 \otimes a^{1/p}$) in the algebra $\mathbb{E}$. Then, $(u, 0)$ and $(u', u - u')$ are **different** Jordan-Chevalley decompositions of u. Moreover there is an u-invariant subspace of $\mathbb{E}$ which is not u'-invariant.

Proof. Note that $q = t^p - a \in \mathbb{K}[t]$ is irreducible over $\mathbb{K}$. Since $u^p = (u')^p$ is the homothety of reason a, we have $q(u) = q(u') = 0$ and hence q is the minimal polynomial of both u and u', which are then semisimple. Clearly $[u, u'] = 0$ and $u \neq u'$. Finally $(u - u')^p = u^p - (u')^p = 0$, so $u - u'$ is non-zero nilpotent.

Set $v = a^{1/p} \otimes 1$ and let $\mathbb{U} = Z(u, v)$. A basis for $\mathbb{U}$ is $v, u(v), \cdots, u^{p-1}(v)$. We leave to the reader to verify that u' sends no element in the above basis to $\mathbb{U}$.

Example 4. Let $\mathbb{K}$ be any field, $\mathbf{V}$ a $\mathbb{K}$-space and $x \in End_{\mathbb{K}}(\mathbf{V})$, such that $dim_{\mathbb{K}}(\mathbf{V}) < \infty$ and the minimal polynomial of x is separable over $\mathbb{K}$. Let (s, n) be the Jordan-Chevalley decomposition of x. Then $(ad(s), ad(n))$ is the unique Jordan-Chevalley decompostion of $ad(x) \in End_{\mathbb{K}}(End_{\mathbb{K}}(\mathbf{V}))$.

Proof. Let L and R be the left and right regular representations of $End_{\mathbb{K}}(\mathbf{V})$. Since $L(n)$ and $R(n)$ are nilpotent and commute, $ad(n) = L(n) - R(n)$ is nilpotent, with $[ad(s), ad(n)] = ad[s, n] = 0$. Moreover, for any $p \in \mathbb{K}[t]$ and $y \in End_{\mathbb{K}}(\mathbf{V})$ we have $L(p(y)) = p(L(y))$ and $R(p(y)) = p(R(y))$, so that $p_s(L(s)) = p_s(R(s)) =$

0, showing that $L(s)$ and $R(s)$ and hence $ad(s) = L(s) - R(s)$, are absolutely semisimple (use Proposition 1.7.2).

Example 5. Let $x, y \in End_{\mathbb{K}}(\mathbf{V})$, $z \in End_{\mathbb{K}}(\mathbf{W})$ such that x, y, z are separable and locally finite, with $[x, y] = 0$. Then $x + y$, xy and $x \otimes z \in End_{\mathbb{K}}(\mathbf{V} \bigotimes \mathbf{W})$ are separable and locally finite and $(x_s + y_s, x_n + y_n)$, $(x_s y_s, x_s y_n + x_n y_s + x_n y_n)$ and $(x_s \otimes z_s, x_s \otimes z_n + x_n \otimes z_s + x_n \otimes z_n)$ are their respective Jordan-Chevalley decompositions.

Proof. Observe that:

(i) $x + y = (x_s + y_s) + (x_n + y_n)$ and $xy = (x_s y_s) + (x_s y_n + x_n y_s + x_n y_n)$.

(ii) $x_s + y_s$ and $x_s y_s$ are absolutely semisimple by Proposition 1.7.2.

(iii) $x_n + y_n$ and $x_s y_n + x_n y_s + x_n y_n$ are locally nilpotent Proposition 1.6.1(ii).

(iv) $[x_s + y_s, x_n + y_n] = 0$ and $[x_s y_s, x_s y_n + x_n y_s + x_n y_n] = 0$ by Proposition 1.6.8.

We have shown that $(x_s + y_s, x_n + y_n)$ and $(x_s y_s, x_s y_n + x_n y_s + x_n y_n)$ are the respective absolute Jordan-Chevalley decompositions of $x + y$ and xy (hence $x + y$ and xy are locally finite and separable).

Note also that:

(v) $1_{\mathbf{V}} \otimes z$ and $x \otimes 1_{\mathbf{W}}$ commute.

(vi) $1_{\mathbf{V}} \otimes z$ and $x \otimes 1_{\mathbf{W}}$ are locally finite and separable. Indeed, for any $v \in \mathbf{V}$, $w \in \mathbf{W}$ and $p \in \mathbb{K}[t]$ we have $p(1_{\mathbf{V}} \otimes z)(v \otimes w) = v \otimes p(z)(w)$ and $p(x \otimes 1_{\mathbf{W}})(v \otimes w) = p(x)(v) \otimes w$. Since $\{v \otimes w | \, v \in \mathbf{V} \text{ and } w \in \mathbf{W}\}$ spans $\mathbf{V} \bigotimes \mathbf{W}$ the assertion readily follows.

(vii) $(x \otimes 1_{\mathbf{W}})_s = x_s \otimes 1_{\mathbf{W}}$, $(x \otimes 1_{\mathbf{W}})_n = x_n \otimes 1_{\mathbf{W}}$, $(1_{\mathbf{V}} \otimes z)_s = 1_{\mathbf{V}} \otimes z_s$ and $(1_{\mathbf{V}} \otimes z)_n = 1_{\mathbf{V}} \otimes z_n$. The proof is immediate.

If we now replace x by $x \otimes 1_{\mathbf{W}}$ and y by $1_{\mathbf{V}} \otimes z$ in the foregoing argument we conclude that $(x_s \otimes z_s, x_s \otimes z_n + x_n \otimes z_s + x_n \otimes z_n)$ is the absolute Jordan-Chevalley decomposition of $x \otimes z$.

Example 6. We present an endomorphism of a finite dimensional space with no Jordan-Chevalley decomposition. One can argue that the smallest dimension of the ambient space $\mathbf{V}$ where this can occur is 4 and that in this case $\mathbb{K}$ must be a

non-perfect field of characteristic 2. Our example is as follows:

Let $\mathbb{K}$ be an imperfect field of characteristic 2 and $a \in \mathbb{K} - \mathbb{K}^2$. Let $\mathbb{V} = \mathbb{K}^4$ and x the endomorphism whose matrix in the canonical basis of $\mathbb{V}$ is

$$A = \begin{pmatrix} 0 & 0 & 0 & a^2 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Then x is cyclic with minimal polynomial $p_x = t^4 + a^2 = (t^2 + a)^2$. Note that $(t^2 + a)$ is irreducible over $\mathbb{K}$ and that $\mathbb{K}[x]$ is four dimensional with basis $1, x, x^2 + a, x(x^2 + a)$, where $(x^2 + a) = J(\mathbb{K}[x])$.

Suppose that x has a Jordan-Chevalley decomposition (s, n). Then

$$0 = (s + n)^4 + a^2 = s^4 + a^2 = (s^2 + a)^2$$

We have used the fact that $[s, n] = 0$ and $n^4 = 0$ (this last holds because n is nilpotent and $dim_{\mathbb{K}}(\mathbb{V}) = 4$. Now from $(s^2 + a)^2 = 0$ and s semisimple we conclude that $p_s = t^2 + a$. Thus $s^2 + a = 0$. We could have also obtained this from Proposition 1.6.1.

Since x is cyclic Proposition 1.6.7 tells us that s is a polynomial in x. Hence

$$s = a_1 + a_2 x + a_3(x^2 - a) + a_4 x(x^2 - a)$$

for unique $a_i \in \mathbb{K}$. Squaring this yields

$$a = s^2 = a_1^2 + a_2^2 x^2$$

Since the minimal polynomial of x has degree four this implies that $a_2 = 0$ and $a = a_1^2$ contradicting the fact that $a \notin \mathbb{K}^2$.

Example 7. This example illustrates Proposition 1.8.3. Let $\mathbb{F}_3$ be the field with 3 elements and A the group algebra $A = \mathbb{F}_3[\mathbf{Z}_6]$. Let a be a generator of the group $\mathbf{Z}_6$. We think of the elements of A as $\mathbb{F}_3$-endomorphisms of A via the regular representation of A. The absolute Jordan-Chevalley decomposition of each of the members of the basis $(a^i)_{0 \leq i \leq 5}$ of A is:

$$1 = 1 + 0$$

$$a = a^3 + (a - a^3)$$

$$a^2 = 1 + (a^2 - 1)$$

$$a^3 = a^3 + 0$$

$$a^4 = 1 + (a^4 - 1)$$

$$a^5 = a^3 + (a^5 - a^3)$$

This is correct since

$$0 = (a^2 - 1)^3 = (a - a^3)^3 = (a^4 - 1)^3 = (a^5 - a^3)^3$$

and a^3 is semisimple with minimal polyomial $t^2 - 1 = (t - 1)(t + 1)$. Now let

$$I = \mathbb{F}_3(a - a^3) \bigoplus \mathbb{F}_3(a^2 - 1) \bigoplus \mathbb{F}_3(a^4 - 1) \bigoplus \mathbb{F}_3(a^5 - a^3)$$

I is an ideal (since $aI \subset I$) and clearly $I \subset J(A)$. But

$$A/I \simeq \mathbb{F}_3[a^3] = \mathbb{F}_3(a^3 - 1) \bigoplus \mathbb{F}_3(1 - (a^3 - 1)) \simeq \mathbb{F}_3 \times \mathbb{F}_3$$

is semisimple, so $I = J(A)$ and $A = \mathbb{F}_3[1, a^3] \bigotimes J(A)$. Thus, as Proposition 1.8.3 shows, $J(A)$ is the ideal generated by the nilpotent parts of elements generating A and $J(A)$ is complemented by the subalgebra generated by the semisimple parts of those elements.

Chapter 2

Separable algebras

This chapter introduces separable algebras and proves some of its basic properties. The connection between separable and classically separable algebras is exploited in the next chapter. The exposition follows DeMeyer-Ingraham [71] and Bass [67].

2.1. Preliminaries

Throughout R will denote a commutative ring with identity. An R-algebra is an R-module with an R-bilinear binary multiplication. We will consider mainly unital associative R-algebras. Accordingly, by A/R being an algebra we will mean that A is an associative unital R-algebra.

The category of associative unital R-algebras is easily seen to be isomorphic to the category whose objects are all pairs (ρ, A), where $\rho: R \to A$ is a central ring homomorphism, with the obvious morphisms between them.

If B is a ring then B^o will denote its opposite ring, that is the ring whose underlying additive abelian group coincides with that of B while its multiplication, denoted by $*$, is defined by $b_1 * b_2 = b_2 b_1$, where $b_2 b_1$ is the product in B. A right B-module is nothing but a representation of B^o.

2.2. $(A-B)/R$ bimodules and left $A \otimes_R B^o$-modules

Definition 2.2.1. *Let A/R , B/R be algebras. An $(A-B)/R$ bimodule is an abelian group M such that:*
BM1. M is an $A-B$ bimodule
BM2. The module structures of M that R inherits from A and B coincide, that is $rm = mr$ for all $r \in R$, $m \in M$.

The following result will give us flexibility in the use of $(A-B)/R$ bimodules.

Lemma 2.2.1. *The categories of $(A-B)/R$ bimodules and left $A \otimes_R B^o$-modules are isomorphic.*

Proof. Indeed, let $R \xrightarrow{\rho} A \xrightarrow{\alpha} End_{\mathbf{Z}}(M) \xleftarrow{\alpha'} B^o \xleftarrow{\rho'} R$ be the ring homomorphisms giving the structure to an $(A-B)/R$ bimodule M.

By BM2 $(\alpha\rho) = (\alpha'\rho')$. Thus there is no confusion in referring to the centralizer of $(\alpha\rho)R = (\alpha'\rho')R$ in $End_{\mathbf{Z}}(M)$ as the R-algebra $End_R(M)$. Note that by BM1 the R-algebra maps $A \xrightarrow{\alpha} End_R(M) \xleftarrow{\alpha'} B^o$ have commuting images.

Due to the universal property of the R-algebra $A \bigotimes_R B^o$, there is a unique R-algebra map from $A \bigotimes_R B^o$ into $End_R(M)$ making the following diagram commutative:

$$\begin{array}{ccccc} & & End_{\mathbf{Z}}(M) & & \\ & & \uparrow & & \\ & & End_R(M) & & \\ & \nearrow & \uparrow & \nwarrow & \\ A & \longrightarrow & A \bigotimes_R B^o & \longleftarrow & B^o \\ & \nwarrow & \uparrow & \nearrow & \\ & & R & & \end{array}$$

We have obtained the desired left $A \bigotimes_R B^o$-module structure for M. It can be read from the diagram that

$$(\sum a_i \otimes b_i)m = \sum (a_i \otimes b_i)m = \sum (a_i \otimes 1)(1 \otimes b_i)m = \sum a_i m b_i$$

whenever $m \in M$, $a_i \in A$, $b_i \in B$.

On the other hand let M be an abelian group and $\gamma\colon A \bigotimes_R B^o \to End_{\mathbf{Z}}(M)$ be a ring homomorphism. Then M becomes a left A-module by pullback along the ring homomorphism $A \to A \bigotimes_R B^o$ defined by $a \to a \otimes 1$ and also a right B-module by pullback along the ring homomorphism $B^o \to A \bigotimes_R B^o$ defined by $b \to 1 \otimes b$. Since

$$(a \otimes 1)(1 \otimes b) = a \otimes b = (1 \otimes b)(a \otimes 1)$$

we see that BM1 is satisfied. Similarly from $r \otimes 1 = 1 \otimes r$ we see that $BM2$ is also satisfied. Note that by definition

$$am = (a \otimes 1)m \text{ and } mb = (1 \otimes b)m$$

for all $m \in M$, $a \in A$, $b \in B$.

In this way, morphisms of one sort become morphism of the other, and following any of these constructions by the other is an identity functor. ♣

An $(A-A)/R$ bimodule will be referred to as an A/R bimodule (= two sided A/R module) and $A \bigotimes_R A^o$ will be denoted by A^e.

2.3. Separable algebras

The concept of **separable** algebra can be formulated in many different, though equivalent, ways. This variety provides a certain degree of freedom at the time of proving some of its basic properties. Before proceeding we will define the main pieces that will appear in the definition.

A simple example of a two sided A/R module is given by A itself. Indeed, the left and right regular representations of A make A into an $A-A$ bimodule and the fact that A is an R-algebra guarantees that $BM2$ is satisfied.

Lemma 2.2.1 now tells us that A becomes a left A^e-module. The action of A^e is given by: $(\sum a_i \otimes b_i)a = \sum a_i a b_i$ for all $a_i, b_i, a \in A$. Another left A^e-module is A^e itself (via its left regular representation). Since $1 \otimes 1$ freely generates A^e as a left A^e-module there is a unique A^e-linear map $\mu\colon A^e \to A$ extending $1 \otimes 1 \to 1$. We have

$$\mu(\sum a_i \otimes b_i) = \sum a_i b_i$$

for all $a_i, b_i \in A$. The kernel of μ will be denoted by J. Thus

(1) $$0 \to J \to A^e \xrightarrow{\mu} A \to 0$$

is exact.

Lemma 1. *J is the left ideal of A^e generated by $\{x \otimes 1 - 1 \otimes x | x \in A\}$.*

Proof. If $x = \sum a_i \otimes b_i \in J$ then:

$x = \sum a_i \otimes b_i - \sum a_i b_i \otimes 1 = -\sum (a_i \otimes 1)(b_i \otimes 1 - 1 \otimes b_i)$. ♣

Definition 1. A **derivation** of A into an A/R bimodule M is an R-linear map $d\colon A \to M$ satisfying the condition: $d(ab) = ad(b) + d(a)b \quad \forall\, a, b \in A$. The set of all such maps will be denoted by $Der(A, M)$. We easily see that $Der(A, M)$ is an R-module.

Given $m \in M$ we can construct a derivation Δ_m of A into M defined by

$$\Delta_m(a) = am - ma$$

Derivations of this form are called **inner**. This gives an R-linear map

$$M \ni m \xrightarrow{\Delta} \Delta_m \in Der(A, M)$$

whose image and kernel are respectively denoted by $\mathrm{Inner}(A, M)$ and

$$M^A = \{m \in M | am = ma \ \forall\, a \in A\} = \{m \in M | (a \otimes 1 - 1 \otimes a)m = 0\}.$$

Note 1. *A^A is the center $Z(A)$ of A and $(A^e)^A$ is the right annihilator of J.*

Note 2. *A derivation followed by an A^e-linear map is again a derivation.*

As explained in Chapter 0 $Hom_{A^e}(J, -)$ is a covariant functor from A^e-Mod to R-Mod. Note 2 essentially tells us that $Der(A, -)$ is also a functor of this kind. Moreover:

Lemma 2. *$Hom_{A^e}(J, -)$ is naturally isomorphic to $Der(A, -)$*

Proof. Let $\delta : A \to A^e$ be the inner derivation corresponding to $1 \otimes 1$, that is, $\delta(a) = a \otimes 1 - 1 \otimes a$. It follows from Lemma 1 that $\delta \in Der(A, J)$. We now use δ to map $Hom_{A^e}(J, M)$ into $Der(A, M)$ as explained in Note 2. More precisely, we define an R-linear monomorphism $Hom_{A^e}(J, M) \ni f \xrightarrow{\delta^*} f\delta \in Der(A, M)$. δ^* is indeed a monomorphism due to Lemma 1.

To see that δ^* is surjective, take any $d \in Der(A, M)$. To get an insight as to what the preimage of d will look like note that if $f\delta = d$ for some $f \in Hom_{A^e}(J, M)$ then whenever $\sum a_i \otimes b_i \in J$ we have:

$$f(\sum a_i \otimes b_i) = f(-\sum (a_i \otimes 1)(b_i \otimes 1 - 1 \otimes b_i)) = -\sum a_i f\delta(b_i) = -\sum a_i d(b_i)$$

where the first equality was shown in Lemma 1 and the second holds since f is an A^e linear map.

Accordingly, we define the R-bilinear map $A \times A^o \ni (a,b) \mapsto -ad(b) \in M$, obtaining an R-linear map satisfying $A^e \ni a \otimes b \mapsto -ad(b) \in M$, whose restriction f to J is A^e-linear and satisfies $f\delta = d$. Indeed, if $\sum a_i \otimes b_i \in J$ and $a, b \in A$ then:

$$f(a \otimes b \sum a_i \otimes b_i) = f(\sum aa_i \otimes b_i b) = -\sum aa_i d(b_i b) = -\sum aa_i (d(b_i)b + b_i d(b)) =$$

$$= -a(\sum a_i d(b_i))b - a(\sum a_i b_i)d(b) = (a \otimes b) f(\sum a_i \otimes b_i) - 0 = (a \otimes b) f(\sum a_i \otimes b_i)$$

and $f\delta(a) = f(a \otimes 1 - 1 \otimes a) = -ad(1) + 1d(a) = d(a)$ where $d(1) = 0$ because d is a derivation. Thus δ^* is an isomorphism. ♣

Lemma 3. *$f \in Hom_{A^e}(J, M)$ can be extended A^e-linearly to A^e iff $f\delta$ is an inner derivation.*

Proof. If f can be extended to A^e then $f\delta$ is the inner derivation corresponding to $f(1 \otimes 1)$, whereas if $f\delta$ is the inner derivation corresponding to $m \in M$ then f is extended to A^e by the unique A^e-linear map satisfying $1 \otimes 1 \mapsto m$. ♣

If $M \xrightarrow{f} N$ is A^e-linear then $f(M^A) \subset N^A$, so that

$$\begin{array}{ccc} M & \to & M^A \\ f & \to & f|_{M^A} \end{array}$$

is a covariant functor F from A^e-Mod to R-Mod. Moreover:

Lemma 4. *F is naturally isomorphic to $Hom_{A^e}(A, -)$.*

Proof. Indeed,

$$\begin{array}{ccc} Hom_{A^e}(A,M) \ni f & \to & f(1) \in M^A \\ M^A \ni m & \to & \widetilde{m} \in Hom_{A^e}(A,M) \end{array}$$

where $\widetilde{m}(a) = am$, are inverse isomorphisms and, moreover, the following diagram commutes:

$$\begin{array}{ccc} Hom_{A^e}(A,M) & \longrightarrow & M^A \\ {\scriptstyle g^*}\downarrow & & \downarrow{\scriptstyle g|_{M^A}} \\ Hom_{A^e}(A,N) & \longrightarrow & N^A \end{array}$$

for any $g \in Hom_{A^e}(M,N)$. ♣

We are ready for:

Definition and Proposition 1. *An A/R algebra is separable if it satisfies the following equivalent conditions:*

1) A is a projective A^e-module.

2) Every derivation of A is inner.

3) $\delta \in Der(A, J)$ is an inner derivation.

4) The functor $M \longrightarrow M^A$ preserves epimorphisms.

5) $(A^e)^A \longrightarrow A^A \longrightarrow 0$ is exact.

6) There exists $e \in A^e$ such that: $\mu(e) = 1$, $Je = 0$.

7) There are $e \in A^e$ and $S \subset A$ satisfying: $\mu(e) = 1$, S spans A as an R-module and $(s \otimes 1 - 1 \otimes s)e = 0$ for all $s \in S$.

8) $Ext^n_{A^e}(A, M) = (0)$ for all A^e-modules M and $n \geq 1$.

For the definition of $Ext^n_{A^e}(A, M)$ please see Jacobson [80], chapter 6. Exact functors and projective modules are explained in Chapter 0.

Proof.

1) $\Rightarrow$ 2) Let M be an A/R bimodule. We have to show that $\Delta\colon M \to Der(A, M)$ is surjective. To see this consider the commutative diagram of R-linear maps:

$$\begin{array}{ccc} M & \xrightarrow{\Delta} & Der(A, M) \\ {\scriptstyle\kappa}\downarrow & & \uparrow{\scriptstyle\delta^*} \\ Hom_{A^e}(A^e, M) & \xrightarrow[\phi]{} & Hom_{A^e}(J, M) \end{array}$$

where κ is the natural isomorphism of A^e-modules $m \to (x \to xm)$, δ^* is the natural isomorphism of Lemma 2 and ϕ is "restriction to J". The bottom line is surjective because J is a direct summand of A^e (the exact sequence (1) splits) and hence so must be the upper line.

2) $\Rightarrow$ 3) Clear.

3) $\Rightarrow$ 1) Apply Lemma 3 to see that the sequence (1) splits. Thus A is isomorphic to a direct summand of a free A^e-module (namely A^e) and hence A is projective by Proposition 0.1.2.

1) $\Longleftrightarrow$ 4) Use Lemma 4 along with Propositions 0.1.1 and 0.1.2.

4) $\Rightarrow$ 5) Clear.

5) $\Rightarrow$ 6) Use Note 1.

6) $\Longleftrightarrow$ 7) Use Lemma 1.

6) $\Rightarrow$ 1) Define $f: A \to A^e$ by $f(a) = (1 \otimes a)e = (a \otimes 1)e$. Direct computation shows that f is A^e-linear and splits (1).

1) $\Longleftrightarrow$ 8) Basic homological property. ♣

Definition and Note 3. *An $e \in A^e$ satisfying 6) is called a* **separability idempotent** *of A. e is idempotent because $e - e^2 = (1 \otimes 1 - e)e \in Je = 0$.* ♣

The equivalence 1) $\Longleftrightarrow$ 8) will not be used in the remainder of this chapter. However it will useful in chapter 3.

2.4. Basic properties of separable algebras

There are many ways to obtain new algebras from old ones, and we will see here that separability is preserved by many of them. We start by introducing two of these constructions.

Note 1. *The following is easy but tedious to check. Let R_i/R be a commutative algebra, A_i/R_i an algebra and M_i a left A_i-module $i = 1, 2$. Then $M_1 \bigotimes_R M_2$ has a unique left $A_1 \bigotimes_R A_2$-module structure such that $\forall m_i \in M_i$, $a_i \in A_i$, $i = 1, 2$:*

$$(a_1 \otimes a_2)(m_1 \otimes m_2) = a_1 m_1 \otimes a_2 m_2.$$

The corresponding statement for right modules also holds and, moreover, application of this procedure to (the R-algebra) $A_1 \bigotimes_R A_2$ yields an $R_1 \bigotimes_R R_2$ algebra with the property that, if M_i is now an A_i/R_i-bimodule, then $M_1 \bigotimes_R M_2$ is an $A_1 \bigotimes_R A_2/R_1 \bigotimes_R R_2$-bimodule.

Note 2. *Let A/R, B/S be algebras defined by central ring homomorphisms $R \xrightarrow{\alpha} A$, $S \xrightarrow{\beta} B$. Suppose we are given ring homomorphisms $R \xrightarrow{f} S$, $A \xrightarrow{g} B$ such that the diagram:*

$$\begin{array}{ccc} A & \xrightarrow{g} & B \\ {\scriptstyle\alpha}\uparrow & & \uparrow{\scriptstyle\beta} \\ R & \xrightarrow[f]{} & S \end{array}$$

commutes. Then any B/S-bimodule M becomes an A/R-bimodule by declaring: $a.m = g(a)m,\ m.a = mg(a)$ *for all* $a \in A,\ m \in M$.

The following general results will be useful in the sequel.

Lemma 1. *Let R_i/R be a commutative algebra and let M_i, N_i be R_i-modules, $i = 1, 2$. There is a natural $R_1 \bigotimes_R R_2$-isomorphism:*

$$(M_1 \bigotimes_R M_2) \bigotimes_{R_1 \bigotimes R_2} (N_1 \bigotimes_R N_2) \xrightarrow{\hat{\psi}} (M_1 \bigotimes_{R_1} N_1) \bigotimes_R (M_2 \bigotimes_{R_2} N_2)$$

where $\hat{\psi}$ is the unique $R_1 \bigotimes_R R_2$-linear map satisfying:

$$(m_1 \otimes m_2) \otimes (n_1 \otimes n_2) \xrightarrow{\hat{\psi}} (m_1 \otimes n_1) \otimes (m_2 \otimes n_2)$$

for all $m_i \in M_i, n_i \in N_i$ $i = 1, 2$. Furthermore if M_i and N_i are R_i-algebras $i = 1, 2$ then $\hat{\psi}$ is an isomorphism of $R_1 \bigotimes_R R_2$-algebras.

Proof.

Denote $(M_1 \bigotimes_R M_2) \bigotimes_{R_1 \bigotimes R_2} (N_1 \bigotimes_R N_2)$ and $(M_1 \bigotimes_{R_1} N_1) \bigotimes_R (M_2 \bigotimes_{R_2} N_2)$ by $\mathcal{X}$ and $\mathcal{Y}$, respectively.

Fix $(m_1, m_2) \in M_1 \times M_2$. Define an R-bilinear map $f^{(m_1,m_2)}: N_1 \times N_2 \to \mathcal{Y}$ by $(n_1, n_2) \to (m_1 \otimes n_1) \otimes (m_2 \otimes n_2)$. By universal nonsense this induces an R-linear map $\hat{f}^{(m_1,m_2)}: N_1 \bigotimes_R N_2 \to \mathcal{Y}$.

This readily gives us a mapping $M_1 \times M_2 \xrightarrow{\theta} Hom_R(N_1 \bigotimes_R N_2, \mathcal{Y})$ defined by $(m_1, m_2) \to \hat{f}^{(m_1,m_2)}$, which is clearly R-bilinear, obtaining then an R-linear map $\hat{\theta}: M_1 \bigotimes_R M_2 \to Hom_R(N_1 \bigotimes_R N_2, \mathcal{Y})$.

The R-bilinear map $(M_1 \bigotimes_R M_2) \times (N_1 \bigotimes_R N_2) \ni (a, b) \xrightarrow{\psi} \hat{\theta}(a)(b) \in \mathcal{Y}$ induced by $\hat{\theta}$ is indeed $R_1 \bigotimes_R R_2$-bilinear. This gives us the desired $R_1 \bigotimes_R R_2$-linear map $\hat{\psi}: \mathcal{X} \to \mathcal{Y}$. Indeed,

$$\hat{\psi}(m_1 \otimes m_2) \otimes (n_1 \otimes n_2) = \hat{\theta}(m_1 \otimes m_2)(n_1 \otimes n_2) = \hat{f}^{(m_1,m_2)}(n_1 \otimes n_2) =$$

$$f^{(m_1,m_2)}(n_1, n_2) = (m_1 \otimes n_1) \otimes (m_2 \otimes n_2).$$

Uniqueness is clear. A similar procedure allow us to construct an arrow reversing $\hat{\psi}$. Now assume that M_i and N_i are R_i-algebras, $i = 1, 2$. Then:

$$\tilde{\psi}((m_1 \otimes m_2) \otimes (n_1 \otimes n_2))((m_1' \otimes m_2') \otimes (n_1' \otimes n_2')) =$$

$$= \hat{\psi}((m_1 \otimes m_2)(m_1' \otimes m_2')) \otimes ((n_1 \otimes n_2)(n_1' \otimes n_2')) = \hat{\psi}(m_1 m_1' \otimes m_2 m_2') \otimes (n_1 n_1' \otimes n_2 n_2') =$$

$$= (m_1 m_1' \otimes n_1 n_1') \otimes (m_2 m_2' \otimes n_2 n_2') = ((m_1 \otimes n_1)(m_1' \otimes n_1')) \otimes ((m_2 \otimes n_2)(m_2' \otimes n_2')) =$$

$$= ((m_1 \otimes n_1) \otimes (m_2 \otimes n_2))((m_1' \otimes n_1') \otimes (m_2' \otimes n_2')).$$

Since $\hat{\psi}$ is an $R_1 \bigotimes_R R_2$-linear isomorphism we see at once that $\hat{\psi}$ is an $R_1 \bigotimes_R R_2$-algebra isomorphism. ♣

Corollary 1.

a) If A_i/R_i is an algebra and R_i/R a commutative algebra $i = 1,2$ then the $R_1 \bigotimes_R R_2$-algebras $(A_1 \bigotimes_R A_2)^e$ and $A_1^e \bigotimes_R A_2^e$ are naturally isomorphic.

b) If S/R is a commutative algebra and A/S an algebra then the S-algebras $(S \bigotimes_R A)^e$ and $S \bigotimes_R A^e$ are naturally isomorphic.

Lemma 2. *Let A_i/R be an algebra and let M_i be left A_i-modules $i = 1,2$. Then*

a) If M_i is A_i projective $i = 1,2$ then $M_1 \bigotimes_R M_2$ is $A_1 \bigotimes_R A_2$ projective.

b) $M_1 \times M_2$ is $A_1 \times A_2$ projective iff M_i is A_i projective $i = 1,2$.

Proof. We make use of Proposition 0.1.2.

(a) Starting from dual basis $(f_i, m_i)_{i \in I}$, $(g_j, n_j)_{j \in J}$ for M_1 and M_2, we construct a dual basis $(f_i \otimes g_j, m_i \otimes n_j)_{(i,j) \in I \times J}$ for $M_1 \otimes M_2$.

(b) If $(f_i, m_i)_{i \in I}$ is a dual basis for $M_1 \times M_2$ then $(f_i|_{M_1 \times (0)}, (1,0)m_i)_{i \in I}$ and $(f_i|_{M_2 \times (0)}, (0,1)m_i)_{i \in I}$ are dual basis for $M_1 \times (0) \simeq M_1$ and $(0) \times M_2 \simeq M_2$, respectively. The other implication follows mutatis mutandis as in (a). ♣

Proposition 1. *If A_i/R_i is an algebra and R_i/R is a commutative algebra such that A_i/R_i is separable and $R_1 \bigotimes_R R_2 \neq 0$, then $A_1 \bigotimes_R A_2/R_1 \bigotimes_R R_2$ is separable.*

We give two proofs.

1^{st} **Proof.** Since A_i is a projective A_i^e-module, Lemma 2 shows that $A_1 \bigotimes_R A_2$ is a projective $A_1^e \bigotimes_R A_2^e \simeq (A_1 \bigotimes_R A_2)^e$ module (the action of $(A_1 \bigotimes_R A_2)^e$ coming from the natural isomorphism $\hat{\psi}$ of Lemma 1 is the one that is needed here).

2^{nd} **Proof.** We have a commutative diagram of $R_1 \bigotimes_R R_2$-homomorphisms:

$$\begin{array}{ccc} A_1^e \bigotimes A_2^e & \xrightarrow{\mu_1 \otimes \mu_2} & A_1 \bigotimes A_2 \\ \hat{\psi}\downarrow & & \| \\ (A_1 \bigotimes A_2)^e & \xrightarrow[\mu]{} & A_1 \bigotimes A_2 \end{array}$$

Let e_i be a separability idempotent for A_i and set $x = \hat{\psi}(e_1 \otimes e_2)$. Then

$$((a_1 \otimes 1) \otimes (a_2 \otimes 1))e_1 \otimes e_2 = ((1 \otimes a_1) \otimes (1 \otimes a_2))e_1 \otimes e_2$$

for all $a_i \in A_i$. Thus applying tha algebra isomorphism $\hat{\psi}$ of Lemma 1 we get

$$(a_1 \otimes a_2) \otimes (1 \otimes 1)x = (1 \otimes 1) \otimes (a_1 \otimes a_2)x$$

By the commutativity of the above diagram we also have

$$\mu(x) = (\mu_1 \otimes \mu_2)(e_1 \otimes e_2) = 1 \otimes 1$$

Hence $A_1 \bigotimes_R A_2 / R_1 \bigotimes_R R_2$ is separable by Proposition 2.3.1(7). ♣

Corollary 2. *If A/R is separable and S/R is a commutative algebra then $A \bigotimes_R S/S$ is separable.*

Proof. Since S is separable over itself ($1 \otimes 1$ is a separability idempotent) it follows from Proposition 1 that $A \bigotimes_R S / R \bigotimes_R S$ is separable. But

$$\begin{array}{ccc} A \bigotimes_R S & = & A \bigotimes_R S \\ \uparrow & & \uparrow \\ R \bigotimes_R S & \longrightarrow & S \end{array},$$

commutes, so the result follows from the more general:

Lemma 3. *Given a commutative diagram of ring homomorphisms,*

$$\begin{array}{ccc} A & \xrightarrow{g} & B \\ {\scriptstyle\alpha}\uparrow & & \uparrow{\scriptstyle\beta} \\ R & \xrightarrow[f]{} & S \end{array}$$

with α, β central and g surjective, if A/R is separable then so is B/S.

Proof. Note 2 shows that every B/S-bimodule becomes an A/R-bimodule in such a way that any exact sequence of B/S-bimodules $M \longrightarrow N \longrightarrow 0$ becomes an exact sequence of A/R-bimodules. Thus $M^A \longrightarrow N^A \longrightarrow 0$ is exact, and since $M^A = M^B$ and $N^A = N^B$, the result follows from Proposition 2.3.1(4). ♣

Corollary 3. *If both f and g above are bijective then A/R separable iff B/S separable.*

Corollary 4. *If S/R is a commutative algebra and A/S an algebra such that A/R separable, then A/S is separable.*

Proof. Set $B = A$ in the Lemma. ♣

Corollary 5. *If A is a separable R-algebra and I is an ideal of R then A/IA is separable R/I-algebra.*

Proof. Set $B = A/IA$ and $S = R/I$ in the Lemma. ♣

Proposition 2. *Let R_i/R be a commutative algebra, A_i/R_i an algebra $i = 1, 2$, such that $A_1 \bigotimes A_2/R_1 \bigotimes R_2$ is separable, A_2 is a faithful R-module and $R.1_{A_2}$ is an R direct summand of A_2. Then A_1/R_1 is separable.*

Proof. Let $M \xrightarrow{f} N \longrightarrow 0$ be an exact sequence of A_1/R_1-bimodules. Note 1 shows how $M \bigotimes A_2$ and $N \bigotimes A_2$ become $A_1 \bigotimes A_2/R_1 \bigotimes R_2$-bimodules.

We have $A_2 = R.1_{A_2} \bigoplus L$, for some R-submodule L of A_2, which allow us to define: $M \times A_2 \ni (m, a_2) \longrightarrow mr \in M$, where $r \in R$, $l \in L$ are unique such that $a_2 = r.1_{A_2} + l$.

This is R-bilinear, inducing an R-linear map $M \bigotimes A_2 \longrightarrow M$ which satisfies $m \otimes (r.1 + l) \longrightarrow mr$, and is easily seen to be an A_1/R_1-bimodule morphism, thus mapping $(M \bigotimes A_2)^{A_1}$, and hence $(M \bigotimes A_2)^{A_1 \otimes A_2}$, into M^{A_1}.

But given $m \in M^{A_1}$, we have $m \otimes 1 \longrightarrow m$ with $m \otimes 1 \in (M \bigotimes A_2)^{A_1 \otimes A_2}$. Hence $(M \bigotimes A_2)^{A_1 \otimes A_2} \twoheadrightarrow M^{A_1}$ is surjective.

The same occurs for N, so that the commutative diagram

$$\begin{array}{ccccc} M \bigotimes A_2 & \xrightarrow{f \otimes 1_{A_2}} & N \bigotimes A_2 & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \\ M & \xrightarrow[f]{} & N & \longrightarrow & 0 \end{array}$$

yields by restriction the commutative diagram

$$\begin{array}{ccccc} (M \bigotimes A_2)^{A_1 \otimes A_2} & \longrightarrow & (N \bigotimes A_2)^{A_1 \otimes A_2} & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \\ M^{A_1} & \longrightarrow & N^{A_1} & \longrightarrow & 0 \end{array}$$

The upper line is exact by hypothesis and vertical arrows surjective as shown before. Therefore the bottom line is also exact. ♣

Corollary 6. *If S/R is a commutative algebra and A/R an algebra, such that S is a faithful R-module, $R.1_S$ is an R direct summand of S and $S \bigotimes A/S$ is separable, then A/R is separable.*

Proof. $S \bigotimes A/S \bigotimes R$ is separable by Corollary 4, so A/R is separable by Proposition 2. ♣

Note 3. The hypothesis of Corollary 6 cannot be relaxed. See Example 12.

Proposition 3. *Let S/R be a separable commutative algebra and A/S a separable algebra. Then A/R is separable.*

Proof. If $M \to N \to 0$ is an exact sequence of A/R-bimodules, then M and N are S/R-bimodules as explained in Note 2. Since S is separable over R, $M^S \to N^S \to 0$ is also exact.

Now observe that M^S and N^S are A/S-bimodules. Indeed, if $m \in M^S, s \in S, a \in A$ then:

$$s(am) = (sa)m = (as)m = a(sm) = a(ms) = (am)s$$

so $am \in M^S$ and similarly $ma \in M^S$. It is clear that BM1 and BM2 hold.

Since A/S is separable $(M^S)^A \to (N^S)^A \to 0$ is exact. But by definition $(M^S)^A = M^A$ and $(N^S)^A = N^A$. The result follows again from Proposition 2.3.1(4). ♣

Proposition 4. *Let R_i/R be a commutative algebra and let A_i/R_i be an algebra $i = 1, 2$. Then:*

(i) $A_1 \times A_2$ is separable over $R_1 \times R_2$ iff A_i/R_i is separable $\quad i = 1, 2$.

(ii) $A_1 \times A_2$ is separable over R iff A_i is separable over $R \quad i = 1, 2$.

Proof.

(i) $A_1 \times A_2$ is separable over $R_1 \times R_2$ iff $A_1 \times A_2$ is $(A_1 \times A_2)^e$ projective iff $A_1 \times A_2$ is $A_1^e \times A_2^e$ projective iff A_i is A_i^e projective $i = 1, 2$ iff A_i/R_i is separable $i = 1, 2$.

The first and fourth equivalences are nothing but the definition of separability. The third one holds due to Lemma 2(b). The second one follows from the following:

Claim. *There is an isomorphism $\omega\colon (A_1 \times A_2)^e \to A_1^e \times A_2^e$ of $R_1 \times R_2$-algebras which is compatible with the actions of $(A_1 \times A_2)^e$ and $A_1^e \times A_2^e$ on $A_1 \times A_2$.*

Proof. First of all observe that $(A_1 \times A_2)^e = (A_1 \times A_2) \otimes_{R_1 \times R_2} (A_1^o \times A_2^o)$. Define ω to be the unique $R_1 \times R_2$-linear extension of

$$(A_1 \times A_2)^e \ni (a_1, a_2) \otimes (b_1, b_2) \to (a_1 \otimes b_1, a_2 \otimes b_2) \in A_1^e \times A_2^e$$

We see at once that ω is an epimorphsim of $R_1 \times R_2$-algebras. In order to see that ω is injective we construct the arrow ϕ reversing ω. There is no problem in verifying the existence (and uniqueness) of group homomorphisms ϕ_1 and ϕ_2 satisfying:

$$A_1^e \ni a_1 \otimes b_1 \xrightarrow{\phi_1} (a_1, 0) \otimes (b_1, 0) \in (A_1 \times A_2)^e$$

$$A_2^e \ni a_2 \otimes b_2 \xrightarrow{\phi_2} (0, a_2) \otimes (0, b_2) \in (A_1 \times A_2)^e$$

Now define $\phi\colon A_1^e \times A_2^e \to (A_1 \times A_2)^e$ by

$$A_1^e \times A_2^e \ni (a, b) \to \phi_1(a) + \phi_2(b) \in (A_1 \times A_2)^e$$

In order to understand why $\phi\omega = 1_{(A_1 \times A_2)^e}$ note that if $a_i, b_i \in A_1$ $i = 1, 2$ then

$$(a_1, 0) \otimes (0, b_2) = (1, 0)(a_1, 0) \otimes (0, b_2) = (a_1, 0) \otimes (1, 0)(0, b_2) = 0$$

$$(0,a_2)\otimes(b_1,0)=(0,1)(0,a_2)\otimes(b_1,0)=(0,a_2)\otimes(0,1)(b_1,0)=0$$

and hence

$$(a_1,a_2)\otimes(b_1,b_2)=((a_1,0)+(0,a_2))\otimes((b_1,0)+(0,b_2))=$$

$$(a_1,0)\otimes(b_1,0)+(0,a_2)\otimes(0,b_2)=\phi\omega(a_1,a_2)\otimes(b_1,b_2).$$

It follows that $\phi\omega=1_{(A_1\times A_2)^e}$, as required. Thus ω is an isomorhsim.

The last statement means that the natural representation of $A_1^e\times A_2^e$ in $A_1\times A_2$ is exactly ω^{-1} followed by the natural representation of $(A_1\times A_2)^e$ in $A_1\times A_2$. A straighforward computation shows that this is true.

(ii) $\Rightarrow$ Use Corollary 4 to see that $A_1\times A_2$ is separable over $R\times R$. Then apply (i).

$\Leftarrow$ Use (i) to see that $A_1\times A_2$ is separable over $R\times R$. Now observe that $R\times R$ is separable over R. Indeed, $e=(1,0)\otimes(1,0)+(0,1)\otimes(0,1)$ is a separability idempotent. It follows from Proposition 3 that $A_1\times A_2$ is separable over R. ♣

2.5. Separable algebras over fields

The next results show that a separable algebra over a field $\mathbb{K}$ is semisimple and finitely generated as a $\mathbb{K}$-space. This need not be the case if the commutative ring R is arbitrary. See Example 12.

Proposition 1. *If A is separable and projective over R, then it is f.g. over R.*

Proof. Let $(f_i,a_i)_{i\in I}$ be a dual basis for A^o over R. For each $i\in I$ let g_i be the left A-linear map from A^e to A obtained by following the homomorphism of left A-modules $A^e\xrightarrow{1_A\otimes f_i}A\bigotimes R$ by the canonical left A-linear map $A\bigotimes R\to A$. Thus $g_i(a\otimes b)=f_i(b)a$ for all a,b. We see at once that $(g_i,1\otimes a_i)$ is a dual basis for A^e as a left A-module. Thus

$$u=\sum_{i\in I_u}g_i(u)(1\otimes a_i)$$

for all $u\in A^e$, where $I_u=\{i\in I/g_i(u)\neq 0\}$ is finite.

Now let e be a separability idempotent for A and replace u in the above equation by $(a \otimes 1)e$, where a is an arbitrary element of A; applying μ we obtain

$$a = \mu((a \otimes 1)e) = \sum_{i \in I_a} g_i((a \otimes 1)e)a_i$$

where I_a stands for $I_{(a\otimes 1)e}$. But since $g_i((a \otimes 1)e) = ag_i(e)$ we see that $I_a \subset I_e$. This added to the fact that $(a \otimes 1)e = (1 \otimes a)e$ yields

$$a = \sum_{i \in I_e} g_i((1 \otimes a)e)a_i$$

Since $e = \sum_{j=1}^{n} x_j \otimes y_j$ for some $x_i, y_i \in A$ we obtain from the above equation that

$$a = \sum_{i \in I_e} (\sum_{j=1}^{n} g_i(x_j \otimes y_j a))a_i = \sum_{i \in I_e} \sum_{j=1}^{n} f_i(y_j a)x_j a_i$$

showing $(x_j a_i)_{1 \leq j \leq n}^{i \in I_e}$ generates A over R. ♣

Corollary 1. *If A is separable over R and R is a semisimple ring then A is f.g. over R. In particular separable algebras over fields are always finite dimensional.*

Proposition 2. *If A/R is separable and M is a left A-module which is projective over R, then M is projective over A.*

Proof. Let $M_1 \longrightarrow M_2 \longrightarrow 0$ be an exact sequence of left A-modules. Since M is R-projective, $Hom_R(M, M_1) \longrightarrow Hom_R(M, M_2) \longrightarrow 0$ is exact.

But $Hom_R(M, M_i)$ can be endowed with an A/R-bimodule structure, namely: $(afb)(m) = af(bm)$ for all $a, b \in A$ and $m \in M$ (all properties easily hold), and by definition $Hom_R(M, M_i)^A = Hom_A(M, M_i)$ $i = 1, 2$.

Since A/R is separable, $Hom_A(M, M_1) \longrightarrow Hom_A(M, M_1) \longrightarrow 0$ is exact. ♣

Corollary 2. *A separable algebra over a semisimple ring is semisimple. In particular separable algebras over fields are semisimple.*

2.6. Separable versus classically separable algebras

The next theorem is the link between the clasical notion of separability for algebras over fields and the modern version treated so far in this chapter. This connection is exploited in the next chapter.

The next preliminary lemma is implicitly used in the theorem.

Lemma 1. *Let A/R be a simple algebra. Then the center of A is a field.*

Proof. Since A has no trivial ideals, A has no trivial A^e-submodules, so $Z(A)=A^A \simeq End_{A^e}(A)$ is a field by Note 2.3.1, Lemma 2.3.4 and Schur's Lemma.♣

Theorem 1. *Let $\mathbb{K}$ be a field and A an $\mathbb{K}$-algebra. The following conditions are equivalent.*

1) A is separable over $\mathbb{K}$.

2) A is classically separable and f.d. over $\mathbb{K}$.

3) There is a field extension $\mathbb{F}$ of $\mathbb{K}$ such that $\mathbb{F} \bigotimes_{\mathbb{K}} A$ is isomorphic to the direct product of a finite number of matrix rings over $\mathbb{F}$, as $\mathbb{F}$-algebra.

4) A is f.d. over $\mathbb{K}$ and isomorphic to the direct product of a finite number of simple $\mathbb{K}$-algebras whose centers are separable over $\mathbb{K}$ (in either sense, by Proposition 1.8.1).

Proof.

1) $\Rightarrow$ 2) A is f.d. over $\mathbb{K}$ by Corollary 2.5.1. If $\mathbb{F}$ is field extension of $\mathbb{K}$ then $\mathbb{F} \bigotimes_{\mathbb{K}} A$ is $\mathbb{F}$-separable by Corollary 2.4.2 and hence semisimple by Corollary 2.5.2. Therefore $J(\mathbb{F} \bigotimes_{\mathbb{K}} A) = (0)$ by Theorem 0.2.1.

2) $\Rightarrow$ 3) Let $\mathbb{F}$ be an algebraic closure of $\mathbb{K}$. Then $\mathbb{F} \bigotimes_{\mathbb{K}} A$ is a finite dimensional $\mathbb{F}$-algebra with no radical, and hence semisimple. By the structure theorem of semisimple algebras, $\mathbb{F} \bigotimes_{\mathbb{K}} A$ is the direct product of a finite number of matrix rings over division $\mathbb{F}$-algebras, which are f.d. over $\mathbb{F}$. Since $\mathbb{F}$ is algebraically closed, 3) follows.

3) $\Rightarrow$ 1) Proposition 2.4.4(ii) and Example 1) below show that $\mathbb{F} \bigotimes_{\mathbb{K}} A$ is separable over $\mathbb{F}$. Therefore $A/\mathbb{K}$ is separable by Corollary 2.4.6.

4) $\Rightarrow$ 1) We have $A \simeq A_1 \times \cdots \times A_n$ where each A_i is a finite dimensional simple

$\mathbb{K}$-algebra whose center is separable over $\mathbb{K}$. We claim that:
(*) *each A_i is separable over its the center C_i.*

Assume for the moment that (*) holds. Then by Proposition 2.4.3 ("transitivity of separability") each A_i is separable over $\mathbb{K}$. We now conclude from Proposition 2.4.4(ii) that A is separable over $\mathbb{K}$, as desired.

To see that (*) holds let $\mathbb{F}$ be any field extension of C_i. It is a well-known result that $\mathbb{F} \bigotimes_{C_i} A_i$ is a (central) simple $\mathbb{F}$-algebra (see Micali [83], Proposition 2.6.5). It follows that A_i is a classically separable C_i algebra . But A_i is finite dimensional over $\mathbb{K}$ and hence over C_i. Thus (*) follows from the implication 2)⇒1).
1) ⇒ 4) A is f.d. over $\mathbb{K}$ by Corollary 2.5.1 and semisimple by Corollary 2.5.2. Hence A is isomorphic to the direct product of a finite number of simple $\mathbb{K}$-algebras. By Proposition 2.4.4(ii) each of these factors is also separable over $\mathbb{K}$, so we are reduced to show:
(**) *the center C of a simple separable (and hence f.d.) $\mathbb{K}$ algebra A is separable over $\mathbb{K}$.*

If (**) is false then $0 < p = char\, C$ and the minimal polynomial q over $\mathbb{K}$ of some $c \in C$ is non-separable. Hence $q(t) = (t^p)^k + a_{k-1}(t^p)^{k-1} + \cdots + a_0$ for some $a_i \in \mathbb{K}$ and $k \in \mathbb{N}$. Let $\mathbb{F}$ be an algebraic closure of $\mathbb{K}$. Since $1, c, \cdots, c^{pk-1}$ are $\mathbb{K}$-linearly independent $1 \otimes 1, 1 \otimes c, \cdots, 1 \otimes c^{pk-1} \in \mathbb{F} \bigotimes_{\mathbb{K}} C$ are $\mathbb{F}$-linearly independent and then so must be $1 \otimes 1, 1 \otimes c, \cdots, 1 \otimes c^k$. Pick f_i in $\mathbb{F}$ such that $f_i^p = a_i$ for each $0 \leq i \leq k-1$ and set

$$\mathbb{F} \bigotimes C \ni n = 1 \otimes c^k + f_{k-1} \otimes c^{k-1} + \cdots + f_0 \otimes 1 \neq 0. \text{ Then}$$

$$n^p = 1 \otimes c^{pk} + 1 \otimes a_i c^{p(k-1)} + \cdots + 1 \otimes a_0 = 1 \otimes (c^{pk} + a_i c^{p(k-1)} + \cdots + a_0) = 0.$$

Since $\mathbb{F} \bigotimes C$ is contained in the center of $\mathbb{F} \bigotimes A$ the non-zero nilpotent element $n \in \mathbb{F} \bigotimes C$ generates a non-zero nilpotent ideal inside $\mathbb{F} \bigotimes A$, contradicting the fact that A is classically separable. ♣

2.7. Examples

1) Let $n \in \mathbb{N}$. Then $M_n(R)$, the R-algebra of $n \times n$ matrices with coefficients in R, is separable over R.

Proof. Denote by e_{ij} the matrix whose entries are all 0 except for the $(i,j)-$th entry which is 1. Now fix j between 1 and n and set $e = \sum_{i=1}^{n} e_{ij} \otimes e_{ji}$.

Then $\mu(e) = \sum_{i=1}^{n} e_{ii} = 1$ and for any $1 \leq k, l \leq n$ we have:
$(e_{kl} \otimes 1 - 1 \otimes e_{kl})e = \sum_{i=1}^{n}(e_{kl}e_{ij} \otimes e_{ji} - e_{ij} \otimes e_{ji}e_{kl}) = e_{kj} \otimes e_{jl} - e_{kj} \otimes e_{jl} = 0$.
Thus $M_n(R)$ is separable over R by Definition 2.3.1(7). ♣

2) Let G be a finite group of order $n \in \mathbf{N}$, such that $n(= n.1_R)$ is a unit in R. Then the group algebra $A = RG$ is R-separable.

Proof. Let $e = 1/n \sum_{g \in G} g^{-1} \otimes g \in A^e$. Then $\mu(e) = 1$ and we have:
$(1 \otimes h)e = 1/n \sum_{g \in G} g^{-1} \otimes gh = 1/n \sum_{l \in G} hl^{-1} \otimes l = (h \otimes 1)e$ for $h \in G$. Thus A is R-separable by Definition 2.3.1(7). ♣

3) If $G \neq (1)$ is a finite group then $A = \mathbf{Z}G$ is not separable over $\mathbf{Z}$.

Proof. First note that for any group H and R-algebra S there is a natural S-algebra isomorphism $RH \bigotimes_R S \to SH$ defined by $\sum r_h.h \otimes s \to \sum (r_h s).h$.

If $\mathbf{Z}G$ is $\mathbf{Z}$ separable, pick a prime $p \in \mathbf{Z}^+$ dividing $\mid G \mid$, so that $\mathbf{Z}G \bigotimes \mathbf{Z}_p \simeq \mathbf{Z}_p G$ is $\mathbf{Z}_p$-separable. Hence $\mathbf{Z}_p G$ is semisimple by Corollary 2.5.2, contradicting the converse of Maschke's Theorem (see Pierce [82], section 3.6). ♣

4) $\mathbf{Q}$ is separable over $\mathbf{Z}$. More generally, if $S \subset R$ is multiplicative then a commutative algebra A over $S^{-1}R$ is $S^{-1}R$-separable iff it is R-separable.

Proof. The usual construction of the tensor product (see Hungerford [74], definition 5.1) gives $A \bigotimes_{S^{-1}R} A = A \bigotimes_R A$. ♣

5) $R[t]$ is not separable over R.

Proof. $R[t]$ is projective and not $f.g.$ over R. ♣

6) Let $\mathbb{K}$ be a field and $g \in \mathbb{K}[t]$. Then $A = \mathbb{K}[t]/(g)$ is $\mathbb{K}$-separable iff $(g, g') = 1$

Proof. Note that if $\mathbb{F}$ is a field extension of $\mathbb{K}$ then $\mathbb{K}[t]/(g) \bigotimes_{\mathbb{K}} \mathbb{F} \simeq \mathbb{F}[t]/(g)$ as

$\mathbb{F}$-algebras. Now apply the Chinese Reminder Theorem and Theorem 2.6.1. ♣

7) An algebra over a perfect field is separable iff it is semisimple and $f.d.$

Proof. Apply Theorem 2.6.1. ♣

8) $\mathbf{C}$ is $\boldsymbol{R}$ but not $\mathbf{Q}$-separable.

Proof. Apply Example 7 and the argument of Example 5, respectively. ♣

9) The quaternion algebra $\mathbb{H}$ over a field $\mathbb{K}$ is separable, when char $\mathbb{K} \neq 2$.

Proof. Put $e = 1/4(1 \otimes 1 - i \otimes i - j \otimes j - k \otimes k)$. Then $\mu(e) = 1$ and we can apply the Definition 2.3.1(7) to $S = \{1, i, j, k\}$ to obtain the result. ♣

10) A subalgebra of a separable algebra is not necessarily separable, not even if the algebra is commutative. For instance, if $\mathbb{K}$ is a field and $x \in M_n(\mathbb{K})$ is not a semisimple endomorphism then $\mathbb{K}[x]$ is a non-separable subalgebra of $M_n(\mathbb{K})$. A counterexample for the commutative case is given by $\mathbf{Q}[i]$ which is a separable $\mathbf{Z}$-algebra. Indeed, $\mathbf{Q}[i]$ is separable over $\mathbf{Q}$ (see Example 6) and $\mathbf{Q}$ is separable over $\mathbf{Z}$ (see Example 4). Thus, $\mathbf{Q}[i]$ is $\mathbf{Z}$-separable (see Proposition 2.4.3) but contains a non-separable $\mathbf{Z}$-subalgebra, namely $\mathbf{Z}[i]$ (see Example 12 below). However, the statement is true for commutative algebras over fields, by Proposition 1.8.1.

11) Let G be a free abelian group of infinite rank and $A = End_{\mathbf{Z}}(G)$. Then A is not separable over $\mathbf{Z}$.

Proof. We can find an infinite $\mathbf{Z}$-linearly independent system inside A. Using the flatness of $\mathbf{Q}$ we see that $A \bigotimes \mathbf{Q}$ contains an infinite $\mathbf{Q}$-linearly independent system. Thus $A \bigotimes \mathbf{Q}$ is not $\mathbf{Q}$-separable by Corollary 2.5.1, so A is not separable over $\mathbf{Z}$. ♣

12) Let $\mathbf{Z}[t] \ni f$ be monic and of degree ≥ 2. Then $A = \mathbf{Z}[t]/(f)$ is separable if and only if the discriminant $D(f)$ of f is a unit in $\mathbf{Z}$ (see Jacobson [74], section 4.8 for the definition of $D(f)$).

Proof. If $D(f)$ is not unit in $\mathbf{Z}$ pick a prime $p \in \mathbf{Z}^+$ dividing D. The canonical ring epimorphsim $\mathbf{Z} \xrightarrow{\pi} \mathbf{Z}_p$ extends uniquely to a ring epimorphism $\mathbf{Z}[t] \to \mathbf{Z}_p[t]$ also

denoted by π. Note that $D(\pi(f)) = \pi(D(f)) = 0 \in \mathbf{Z}_p$. Hence $(\pi(f), \pi(f)') \neq 1$, so $A \bigotimes \mathbf{Z}_p \simeq \mathbf{Z}_p[t]/(\pi(f))$ is not separable over $\mathbf{Z}_p$, by Example 6, and hence A is not separable over $\mathbf{Z}$.

As for the converse, if $D(f)$ is unit in $\mathbf{Z}$ let $p \in \mathbf{Z}^+$ be any prime. Then $D(\pi(f)) = \pi(D(f))$ is a unit in $\mathbf{Z}_p$ and therefore $(\pi(f), \pi(f)') = 1$, obtaining that $A/pA \simeq \mathbf{Z}_p[t]/(\pi(f)) \simeq \mathbf{Z}[t]/(f) \bigotimes \mathbf{Z}_p$ is $\mathbf{Z}_p$-separable by Example 6. Since f is monic A is f.g. over $\mathbf{Z}$. Hence A is $\mathbf{Z}$-separable due to the following result:
DeMeyer-Ingraham [71], Theorem 7.1. *Let A be a f.g. algebra over R. If A/mA is R/m-separable for every maximal ideal m of R then A is separable over R.* ♣

Remark. The hypothesis of Corollary 2.4.6 can not be relaxed.
(i) Take $A = \mathbf{Z}[t]/(t^2 + 1)$, $R = \mathbf{Z}$ and $S = \mathbf{Z}_5 = \mathbf{Z}/5\mathbf{Z}$. Then $R.1_S = S$ is an R-direct summand of S but S is not a faithful R-module. In this case $S \bigotimes A \simeq \mathbf{Z}_5[t]/(t^2 + 1)$ is a separable $\mathbf{Z}_5$-algebra (see Example 7), but $A = \mathbf{Z}[i]$ is not a separable $\mathbf{Z}$-algebra.
(ii) Let $G \neq (1)$ be any finite group. Let $R = \mathbf{Z}$ and take A to be the group algebra $\mathbf{Z}G$. If $S = \mathbf{Q}$ then S is a faithful R-module but $R.1_S$ is not a direct summand of $\mathbf{Q}$ (which is an indecomposable $\mathbf{Z}$-module). In this case $S \bigotimes A \simeq SG$ is separable over S (see Example 2) but A is not separable over R (see Example 3).

Remark. A separable algebra A over an arbitrary commutative ring need not be semisimple or f.g. as an R-module.
(i) R is always separable over itself, $1 \otimes 1$ being a separability idempotent.
(ii) $\mathbf{Q}$ is separable (see Example 4) but not f.g. over $\mathbf{Z}$.

Chapter 3

Extension of algebras

This chapter studies extension of algebras and proves Wedderburn-Malcev Theorem. Necessary tools for this task are developed in the first section, in which we follow Jacobson [80]. The last two sections are based on Hochschild [45].

3.1. Hochschild cohomology modules of an algebra

We still denote by R a commutative ring with identity, while A will denote an associative unital R-algebra which projective as an R-module. Since A is naturally a two sided A/R-module, A also is a left A^e-module. The notions of homological algebra required for this section can be found in Jacobson [80], chapter 6.

Given a left A^e-module M, the n-th cohomology module of A with coefficients in M is defined to be $Ext^n_{A^e}(A,M)$, while the n-th Hochschild cohomology module $H^n(A,M)$ of A with coefficients in M is the n-th homology module of the complex

$$0 \to C^0(A,M) \xrightarrow{\delta_1} C^1(A,M) \xrightarrow{\delta_2} C^2(A,M) \to \cdots$$

where $C^n(A,M)$ is the R-module of R-multilinear maps from A^n into M $n \geq 1$, $C^0(A,M) = M$ and the R-linear maps $\delta_{n+1}\colon C^n(A,M) \to C^{n+1}(A,M)$ $n \geq 1$ are defined by $(\delta_{n+1}(g))(a_1, \cdots, a_{n+1}) =$

$$a_1 g(a_2, \cdots, a_{n+1}) + \sum_{i=1}^{n} (-1)^i g(a_1, \cdots, a_i a_{i+1}, \cdots, a_{n+1}) + (-1)^{n+1} g(a_1, \cdots, a_n) a_{n+1}$$

while $(\delta_1 m)(a) = am - ma$

In this section we show that

(I) $$Ext^n_{A^e}(A,M) \simeq H^n(A,M) \text{ for all } n \geq 0.$$

This fact will used in section 3.3.

We start by defining a projective resolution for A that will allow us to obtain the desired isomorphisms (I). Let

$$X_0 = A \otimes_R A,\ X_1 = A \otimes_R A \otimes_R A, \cdots,\ X_n = \underbrace{A \otimes_R \cdots \otimes_R A}_{n+2 \text{ times}}$$

Observe that each X_n has a unique left A^e-module structure satisfying

$$(a \otimes b)(a_0 \otimes a_1 \otimes \cdots \otimes a_{n+1}) = aa_0 \otimes a_1 \otimes \cdots \otimes a_{n+1}b$$

for all a, b, a_i in A.

We now prove that X_n is a projective A^e-module for all $n \geq 0$. To see this, we first show

$$X_o \simeq A^e,\ X_1 \simeq A^e \bigotimes_R A,\ X_n \simeq A^e \bigotimes_R X_{n-2} \quad n \geq 2$$

as A^e-modules.

We start by the case $n \geq 2$. In this case the R-multilinear map:

$$A^{n+2} \ni (a_o, a_1, \cdots, a_{n+1}) \mapsto (a_o \otimes a_{n+1}) \otimes (a_1 \otimes \cdots \otimes a_n) \in A^e \bigotimes X_{n-2}$$

induces a unique R-linear map $\lambda_n \colon X_n \to A^e \bigotimes X_{n-2}$ satisfying

$$X_n \ni a_o \otimes a_1 \otimes \cdots \otimes a_{n+1} \mapsto (a_o \otimes a_{n+1}) \otimes (a_1 \otimes \cdots \otimes a_n) \in A^e \bigotimes X_{n-2}$$

which is clearly surjective.

It is also injective, for we can construct R-linear maps:

$$\begin{array}{ccccc} A^e \bigotimes X_{n-2} & \to & X_n & \to & X_n \\ (a_o \otimes a_{n+1}) \otimes (a_1 \otimes \cdots \otimes a_n) & \mapsto & a_o \otimes a_{n+1} \otimes \cdots \otimes a_n & \mapsto & a_o \otimes a_1 \otimes \cdots \otimes a_{n+1} \end{array}$$

that following λ_n give the identity in X_n.

Finally, λ_n is A^e-linear, which by additivity, we only need to check on generators:

$$(a \otimes b)(a_o \otimes \cdots \otimes a_{n+1}) = aa_o \otimes \cdots \otimes a_{n+1}b \mapsto$$

$$(aa_o \otimes a_{n+1}b) \otimes (a_1 \otimes \cdots \otimes a_n) = (a \otimes b)((a_o \otimes a_{n+1}) \otimes (a_1 \otimes \cdots \otimes a_n)).$$

If $n = 1$ the same idea applies, and if $n = 0$ the assertion is clear.

Using Lemma 2.4.2(a) properly, we see that $A, , X_o, X_1, \cdots$ are projective R-modules, and that this implies that A^e, $A^e \bigotimes A$, $A^e \bigotimes X_o$, $A^e \bigotimes X_1, \cdots$, and hence X_o, X_1, X_2, $X_3, \cdots$, are indeed projective A^e-modules, as desired.

We now use the X_n's to provide a projective resolution for A, as A^e-module. First define the A^e-linear map $d_o\colon X_o \to A$ by

$$\sum a_i \otimes b_i \to \sum a_i b_i$$

and for $n > 0$ define $d_n\colon X_n \to X_{n-1}$ to be the unique R-linear map extending:

$$a_o \otimes \cdots \otimes a_{n+1} \to \sum_{i=0}^{n} (-1)^i a_o \otimes \cdots \otimes a_i a_{i+1} \otimes \cdots \otimes a_{n+1}$$

We easily see that the d_n's are morphism of two sided A/R-modules, and hence A^e-linear maps.

We claim that the sequence

$$\text{(P)} \qquad 0 \leftarrow A \xleftarrow{d_o} X_o \xleftarrow{d_1} X_1 \xleftarrow{d_2} X_2 \leftarrow \cdots$$

is exact. To see this we define R-linear maps:

$$A \xrightarrow{s_{-1}} X_o \xrightarrow{s_o} X_1 \xrightarrow{s_1} X_2 \to \cdots$$

where $s_{-1}(a) = 1 \otimes a$ and $s_n\colon X_n \to X_{n+1}$ is the unique R-linear map extending:

$$a_o \otimes \cdots \otimes a_{n+1} \to 1 \otimes a_o \otimes \cdots \otimes a_{n+1}.$$

We easily see that these maps satisfy:

(1) $d_o s_{-1} = 1_A$ and $s_{n-1} d_n + d_{n+1} s_n = 1_{X_n}$ $n \geq 0$.

(2) X_o is A^e-generated by $s_{-1}(A)$ and X_{n+1} is A^e-generated by $s_n(X_n)$ $n \geq 0$.

(3) $d_o d_1 = 0$.

Moreover, assume that $k \geq 0$ and that $d_n d_{n+1} = 0$ for all $n \leq k$. Then by (1)

$$d_{k+1} d_{k+2} s_{k+1} = d_{k+1}(1 - s_k d_{k+1}) = d_{k+1} - (1 - sk - 1 d_k) d_{k+1} = s_{k-1} d_k d_{k+1} = 0.$$

Hence $d_{k+1} d_{k+2} = 0$ because of (2). It now follows from (3) and our inductive argument that (P) is a complex. Furthermore (1) says that $(s_i)_{(i \geq -1)}$ is a homotopy between the identity and the zero maps of the complex (P), which are then equal in homology. Hence (P) is indeed exact, as desired.

Now given an A/R bimodule M we apply $Hom_{A^e}(-, M)$ to (P) to obtain the complex of R-modules:

$$0 \to Hom_{A^e}(X_o, M) \xrightarrow{d_1^*} Hom_{A^e}(X_1, M) \xrightarrow{d_2^*} Hom_{A^e}(X_2, M) \xrightarrow{d_3^*} \cdots$$

Our final step is to construct R-linear maps $\delta_{n+1} : C^n(A, M) \to C^{n+1}(A, M)$ $n \geq 0$ and R-isomorphisms $Hom_{A^e}(X_n, M) \xrightarrow{\psi_n} C^n(A, M) \quad n \geq 0$, such that:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Hom_{A^e}(X_o, M) & \xrightarrow{d_1^*} & Hom_{A^e}(X_1, M) & \xrightarrow{d_2^*} & Hom_{A^e}(X_2, M) & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle \psi_o} & & \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_2} & & \\
0 & \longrightarrow & C^o(A, M) & \xrightarrow[\delta_1]{} & C^1(A, M) & \xrightarrow[\delta_2]{} & C^2(A, M) & \longrightarrow & \cdots
\end{array}$$

is an isomorphism of chain complexes.

When $n \geq 1$, let

$$Hom_{A^e}(X_n, M) \ni f \xrightarrow{\psi_n} \widehat{f} \in C^n(A, M),$$

where

$$\widehat{f}(a_1, \cdots, a_n) = f(1 \otimes a_1 \otimes \cdots \otimes a_n \otimes 1).$$

$\widehat{f}$ is evidently R-multilinear, and ψ_n is clearly R-linear.

In the other direction define:

$$C^n(A, M) \ni g \xrightarrow{\omega_n} \widetilde{g} \in Hom_{A^e}(X_n, M),$$

where $\widetilde{g}$ is the unique R-linear extension of

$$a_o \otimes \cdots \otimes a_{n+1} \to a_o g(a_1, \cdots, a_n) a_{n+1}.$$

We see at once that $\widetilde{g}$ is A^e-linear, and that ω_n R-linear. These maps are inverse isomorphisms. Indeed:

$$\widetilde{\widehat{f}}(a_o \otimes \cdots \otimes a_{n+1}) = a_o \widehat{f}(a_1, \cdots, a_n) a_{n+1} =$$

$$a_o f(1 \otimes a_1 \cdots \otimes a_n \otimes 1) a_{n+1} = f(a_o \otimes \cdots \otimes a_{n+1})$$

and also

$$\widetilde{\widehat{f}}(a_1,\cdots,a_n)=\widehat{f}(1\otimes a_1\otimes\cdots\otimes a_n\otimes 1)=f(a_1,\cdots,a_n).$$

The R-isomorphisms ψ_0 and ω_0 are defined:

$$Hom_{A^e}(X_o,M)\ni f \xrightarrow{\psi_0} f(1\otimes 1)\in M$$

$$M\ni m \xrightarrow{\omega_0} \overline{m}\in Hom_{A^e}(X_o,M)$$

where $\overline{m}(\sum a_1\otimes b_i)=\sum a_1 m b_i$. They are clearly inverse R-isomorphisms. There is now only one way define the δ_n's. Namely, $(\delta_1 m)(a)=(\psi_1 d_1^*\omega_0)(m)(a)=am-ma$ for all $m\in M, a\in A$, and

$$(\delta_{n+1}(g))(a_1,\cdots,a_{n+1})=((\psi_{n+1}d_{n+1}^*\omega_n)(g))(a_1,\cdots,a_{n+1})=$$

$$a_1 g(a_2,\cdots,a_{n+1})+\sum_{i=1}^{n}(-1)^i g(a_1,\cdots,a_i a_{i+1},\cdots,a_{n+1})+(-1)^{n+1}g(a_1,\cdots,a_n)a_{n+1}$$

for all $n\geq 1$, $g\in C^n(A,M)$, $a_i\in A$, as direct computation shows.

We have obtained the promised complex isomorphism. If we now set

$$Z^n(A,M)=\ker\delta_{n+1} \qquad \text{and} \qquad B^n(A,M)=\delta_n C^n(A,M)$$

for all $n\geq 0$ (where $\delta_0=0$), then we have shown that

$$H^n(A,M)=Z^n(A,M)/B^n(A,M)\simeq Ext^n_{A^e}(A,M)$$

as announced at the beginning of the section.

An element of $H^n(A,M)$ will be referred to as an (n,M)-cohomology class of A. Note that, by definition:

$Z^0(A,M)=\{m\in M/am=ma \quad \forall a\in A\}=M^A$.

$Z^1(A,M)=\{f\in C^1(A,M)/f(a_1a_2)=a_1f(a_2)+f(a_1)a_2\}=Der(A,M)$.

$Z^2(A,M)=\{f\in C^2(A,M)/a_1f(a_2,a_3)-f(a_1a_2,a_3)+f(a_1,a_2a_3)-f(a_1,a_2)a_3=0\}$.

$B^1(A,M)=\{f\in C^1(A,M)/\exists m\in M\colon f(a)=am-ma\}=Inner(A,M)$.

$B^2(A,M)=\{f\in C^2(A,M)/\exists g\in C^1(A,M)\colon f(a_1,a_2)=a_1g(a_2)-g(a_1a_2)+g(a_1)a_2\}$.

3.2. Extensions of algebras

Let R be a commutative ring and A an associative unital algebra. Throughout we assume that A is projective as an R-module.

An **extension** of A is a pair (B, σ) where B is an associative R-algebra and $\sigma\colon B \to A$ an R-algebra epimorphism. We will denote $\ker \sigma$ by N.

This extension is called: **Unital** if B is unital, **singular** if $N^2 = (0)$, **split** if there is an R-algebra map $\rho\colon A \to B$ such that $\sigma\rho = 1_A$ and **linearly unital** if the following two conditions are satisfied:

LU1. There is an R-linear map $\rho\colon A \to B$ such that $\sigma\rho = 1_A$.

LU2. $\rho(1_A)n = n\rho(1_A) = n$ for all $n \in N$.

Two extensions (B, σ), $(B^*\sigma^*)$ are **equivalent** if there is an R-algebra isomorphism $I\colon B \to B^*$ such that $\sigma^* I = \sigma$. This fact will be denoted by $(B, \sigma) \backsim (B^*\sigma^*)$.

Proposition 1. *Let (B, σ) and $(B^*\sigma^*)$ be extensions of A.*

1) If $(B, \sigma) \backsim (B^*, \sigma^*)$ via I, then:

(a) $I(N) = N^* = \ker \sigma^*$.

(b) (B, σ) is unital (resp. singular, split and linearly unital) iff (B^*, σ^*) is unital (resp. singular, split and linearly unital).

2) If (B, σ) is singular and unitary, then it is linearly unital.

3) (B, σ) splits iff $B = A^* \bigoplus N$ (as R-modules) for some subalgebra A^* of B, which is then isomorphic to A.

Proof.

1) Clear.

2) Since A is projective there is an R-linear map $\rho\colon A \to B$ satisfying $\sigma\rho = 1_A$. Then $(\rho(1_A) - 1_B)n = n(\rho(1_A) - 1_B) = 0$ for all $n \in N$ because $\rho(1_A) - 1_B \in N$ and $N^2 = (0)$.

3) If there is an R-algebra map $\rho\colon A \to B$ such that $\sigma\rho = 1_A$ then:

(i) $\rho\sigma = (\rho\sigma)^2$, that is, $\rho\sigma = (\rho\sigma)^2$ is a projection of B.

(ii) The image of $\rho\sigma$ is a subalgebra A^* of B.

(iii) The kernel of $\rho\sigma$ is $\ker\sigma = N$.

It follows that $B = A^* \bigoplus N$. Conversely, given $a \in A$ there is a unique $a^* \in A^*$ such that $\sigma(a^*) = a$. Then $a \xrightarrow{\rho} a^*$ is an algebra map and $\sigma\rho = 1_A$. ♣

3.3. Singular extensions and 2-cohomology classes of an algebra

Let (B, σ) a singular and linearly unital extension of A. We show how (B, σ) uniquely determines a structure of two sided A/R-module on $N = \ker\sigma$.

We pick an R-linear map $\rho\colon A \to B$ satisfying LU1 and LU2 and set:

$$a.n = \rho(a)n \qquad n.a = n\rho(a)$$

for all $a \in A$ and $n \in N$. We claim that this defines a structure of two sided A/R-module on $N = \ker\sigma$ and moreover, that the action of R on N remains unchanged. Indeed, if $a_1, a_2 \in A$, $n \in N$ and $r \in R$ then

$$a_1(a_2n) = \rho(a_1)\rho(a_2)n \quad \text{and} \quad (a_1a_2)n = \rho(a_1a_2)n$$

Since $\rho(a_1a_2) - \rho(a_1)\rho(a_2) \in N$ and $N^2 = (0)$ the above expressions are equal. We also have

$$r.n = \rho(r)n = \rho(r.1_A)n = r\rho(1_A)n = rn$$

since ρ satisfies LU2.

It is shown similarly that the analogous relations hold from the right and the remaining properties are easily checked. The claim is proven.

The structure just defined on N depends only on (B, σ). Indeed, if $\rho'\colon A \to B$ is also R-linear and merely satisfies LU1, then $\sigma(\rho - \rho') = 0$, so $(\rho - \rho')(A) \subset N$. Since $N^2 = 0$, the assertion follows.

We also show how (B, σ) uniquely determines a $(2, N)$-cohomology class of A.

The map $f_\rho\colon A \times A \to N$ defined by

$$f_\rho(a_1, a_2) = \rho(a_1)\rho(a_2) - \rho(a_1a_2)$$

is R-bilinear and does take values in N because of LU1 and $N^2 = 0$. Furthermore, $f_\rho \in Z^2(A, N)$. Indeed,

$$(\delta_3 f)(a_1, a_2, a_3) = a_1.f(a_2, a_3) - f(a_1a_2, a_3) + f(a_1, a_2a_3) - f(a_1, a_2).a_3 =$$

$$\rho(a_1)\rho(a_2)\rho(a_3) - \rho(a_1)\rho(a_2a_3) + \rho(a_1a_2a_3) - \rho(a_1a_2)\rho(a_3) -$$

$$\rho(a_1a_2a_3) + \rho(a_1)\rho(a_2a_3) + \rho(a_1a_2)\rho(a_3) - \rho(a_1)\rho(a_2)\rho(a_3) = 0.$$

Moreover if $\rho' \colon A \to B$ is another R-linear which satisfies LU1, then we have $f_\rho - f_{\rho'} = \delta_2(\rho - \rho')$. Indeed, $(f_\rho - f_{\rho'})(a_1, a_2) =$

$$\rho(a_1)\rho(a_2) - \rho(a_1a_2) + \rho'(a_1)\rho(a_2) - \rho'(a_1)\rho(a_2) - \rho'(a_1)\rho'(a_2) + \rho'(a_1a_2) =$$

$$\rho'(a_1)(\rho - \rho')(a_2) - (\rho - \rho')(a_1a_2) + (\rho - \rho')(a_1)\rho(a_2) =$$

$$a_1.(\rho - \rho')(a_2) - (\rho - \rho')(a_1a_2) + (\rho - \rho')(a_1).a_2 = (\delta_2(\rho - \rho'))(a_1, a_2)$$

We have shown therefore that our extension (B, σ) uniquely determines the $(2, N)$-cohomology class $f_\rho + B^2(A, N)$ of A.

We now demonstrate that the two sided A/R-module N and 2-cohomology class $f_\rho + B^2(A, N)$ of A just defined are essentially determined by any of the extensions equivalent to (B, σ).

If $(B, \sigma) \backsim (B^*, \sigma^*)$ via I, then $\rho^* = I\rho$ satisfies LU1 and LU2 with respect to (B^*, σ^*), thus defining on $N^* = \ker \sigma^*$ the two sided A/R-module structure which corresponds to (B^*, σ^*), and we claim that the restriction φ of I to N, $\varphi \colon N \to N^*$, is an isomorphism of two sided A/R-modules.Indeed,

$$\varphi(a.n) = \varphi(\rho(a)n) = \varphi\rho(a)\varphi(n) = \rho^*(a)\varphi(n) = a.\varphi(n)$$

for all $a \in A, n \in N$. Moreover, since $\varphi f_\rho = If_\rho = f_{I\rho} = f_{\rho^*}$, the R-linear map $H^2(\varphi) \colon H^2(A, N) \to H^2(A, N^*)$ which is defined by $H^2(\varphi)(g + B^2(A, N) = \varphi g + B^2(A, N^*)$ sends $f_\rho + B^2(A, N)$ to $f_{\rho^*} + B^2(A, N^*)$, proving that the class of (B, σ) uniquely determines the class of $(N, f_\rho + B^2(A, N))$ in the following sense:

Definition 1. *A pair $(M, f + B^2(A,M))$, where M is a two sided A/R-module and $f \in Z^2(A,M)$, henceforth called a* **2-cohomology pair** *of A, is equivalent to another such a pair $(N, g + B^2(A,N))$ if there is an isomorphism of two sided A/R-modules $\varphi\colon M \to N$ such that $\varphi f + B^2(A,M) = g + B^2(A,N)$.*

We have then constructed a correspondence from the class $\mathcal{A}$ of equivalence classes of singular and linearly unital extensions of A to the class $\mathcal{B}$ of equivalence classes of 2-cohomology pairs of A. We now show how to construct the inverse correspondence.

Given a 2-cohomology pair $(M, f + B^2(A,M))$, let B be the R-space $A \times M$. Define a binary operation on B by

$$(a_1, m_1)(a_2, m_2) = (a_1a_2, a_1m_2 + m_1a_2 + f(a_1, a_2)).$$

We claim that with this multiplication B becomes an associative (not necessarily unital) R-algebra. The fact that the product above is R-bilinear is immediate. Associativity follows from $f \in Z^2(A,M)$. Indeed,

$$((a_1, m_1)(a_2, m_2))(a_3, m_3) =$$

$$(a_1a_2a_3, a_1a_2m_3 + a_1m_2a_3 + m_1a_2a_3 + f(a_1, a_2)a_3 + f(a_1a_2, a_3))$$

and $(a_1, m_1)((a_2, m_2)(a_3, m_3)) =$

$$(a_1a_2a_3, a_1a_2m_3 + a_1m_2a_3 + a_1f(a_2, a_3) + m_1a_2a_3 + f(a_1, a_2a_3))$$

are equal because $f \in Z^2(A,M)$. We thus obtain an associative R-algebra B_f.

Now $\sigma\colon B_f \to A$ defined by $\sigma(a,m) = a$ is an R-algebra epimorphism with kernel $N = (0) \times M$ satisfying $N^2 = (0)$. Thus (B_f, σ) is a singular extension of A. Moreover, let $\rho\colon A \to B_f$, $\rho(a) = (a, 0)$. Then ρ is R-linear, $\sigma\rho = 1_A$ and $n\rho(1) = \rho(1)n = n$ for all $n \in N$, so (B_f, σ) is a linearly unital extension.

The extension just constructed is essentially independent of the choice of the representative f. Indeed, if $f - g = \delta_2 h$ for some $h \in C^1(A,M)$, we then define

$I\colon B_f \to B_g$ by $I(a,m) = (a, m + h(a))$. I is clearly an R-isomorphism, $\sigma I = \sigma$, and we check that I is an R-algebra isomorphism. Indeed,

$$I((a_1,m_1)(a_2,m_2)) =$$

$$I(a_1a_2, a_1m_2 + m_1a_2 + f(a_1,a_2)) = (a_1a_2, a_1m_2 + m_1a_2 + f(a_1,a_2) + h(a_1a_2)) =$$

$$(a_1a_2, a_1m_2+m_1a_2+a_1h(a_2)+h(a_1)a_2+g(a_1,a_2)) = (a_1, m_1+h(a_1))(a_2, m_2+h(a_2)) =$$

$$I(a_1,m_1)I(a_2,m_2).$$

Hence $(B_f,\sigma) \backsim (B_g,\sigma)$ via I.

Now in general, if $(M', f' + B^2(A,M')) \backsim (M, f + B^2(A,M))$ via φ, we then define $I\colon A \times M' \to A \times M$ by $I(a,m') = (a,\varphi(m'))$. It is evident that I is an R-linear isomorphism, and in fact an R-algebra isomorphism from $B_{f'}$ onto $B_{\varphi f'}$:

$$I(a_1,m_1')(a_2,m_2') = I(a_1a_2, a_1m_2' + m_1'a_2 + f'(a_1,a_2)) =$$

$$(a_1a_2, a_1\varphi(m_2') + \varphi(m_1')a_2 + (\varphi f')(a_1,a_2)) = (a_1,\varphi(m_1'))(a_2,\varphi(m_2')) =$$

$$I(a_1,m_1')I(a_2,m_2')$$

Since we also have $\sigma I = \sigma'$ we have shown that

$$(B_{f'},\sigma') \backsim (B_{\varphi f'},\sigma) \backsim (B_f,\sigma).$$

This gives the promised correspondence from $\mathcal{B}$ to $\mathcal{A}$, and we now verify that these two constructions are inverse of each other.

Given $(M, f+B^2(A,M))$ construct (B_f,σ) and then pick $\rho\colon A \to A\times M$ defined by $\rho(a) = (a,0)$ as an R-linear map satisfying LU1 and LU2. Observe that the kernel N of σ is $N = (0) \times M$.

We claim that $(M, f + B^2(A,M)) \backsim (N, f_\rho + B^2(A,N))$. To see this define the mapping $\varphi\colon M \to N$ given by $\varphi(m) = (0,m)$. We have:
(i) φ is a homomorphism of isomorphism of two sided A/R-modules. Indeed, φ is clearly additive. Moreover if $a \in A$ and $m \in M$ then

$$\varphi(a.m) = (0,am) = (a,0)(0,m) = \rho(a)(0,m) = a.(0,m) = a.\varphi(m)$$

and the similar equality holds from the right.

(ii) $\varphi f = f_\rho$. Indeed,

$$f_\rho(a_1, a_2) = \rho(a_1)\rho(a_2) - \rho(a_1 a_2) =$$

$$(a_1 a_2, f(a_1, a_2)) - (a_1 a_2, 0) = (0, f(a_1, a_2)) = \varphi f(a_1, a_2)$$

We have proved the desired relation $(M, f + B^2(A, M)) \backsim (N, f_\rho + B^2(A, N))$.

Finally, given a singular and linearly unital extension (B, σ) pick an R-linear map $\rho\colon A \to B$ satisfying LU1 and LU2 to obtain a 2-cohomology pair $(N, f_\rho + B^2(A, N))$, where $N = \ker \sigma$. From this pair we obtain the extension (B_{f_ρ}, σ') of A, where $B_{f_\rho} = A \times N$ and $\sigma'(a, n) = a$ for all $a \in A$.

We claim that $(B_{f_\rho}, \sigma') \backsim (B, \sigma)$. To see this define the mapping $I\colon B_{f_\rho} \to B$ by $I(a, n) = \rho(a) + n$. From the fact that $\rho\sigma$ is a projection of B with kernel N and image $\rho(A)$ we deduce that I is an R-linear isomorphism. Moreover,

$$I(a_1, n_1)(a_2, n_2) = I(a_1 a_2, a_1 n_2 + n_1 a_2 + \rho(a_1)\rho(a_2) - \rho(a_1 a_2)) =$$

$$a_1 u_2 + u_1 a_2 + \rho(a_1)\rho(a_2) = \rho(a_1) n_2 + n_1 \rho(a_2) + \rho(a_1)\rho(a_2) =$$

$$(\rho(a_1) + n_1)(\rho(a_2) + n_2) = I(a_1, n_1) I(a_2, n_2)$$

Since we also have $(\sigma I)(a, n) = \sigma(\rho(a) + n) = a = \sigma'(a, n)$ the desired relation $(B_{f_\rho}, \sigma') \backsim (B, \sigma)$ is established.

Thus, we have proved:

Proposition 1. *There is a one to one correspondence from the class $\mathcal{A}$ of equivalence classes of singular and linearly unital extensions of A onto the class $\mathcal{B}$ of equivalence classes of 2-cohomology pairs of A.* ♣

We use this result to demonstrate:

Proposition 2. *A singular and linearly unital extension of A is split iff its corresponding 2-cohomology class is zero.*

Proof. We prove sufficiency in two different ways.

$\Rightarrow$ If (B,σ) splits through an R-algebra map ρ then $f_\rho = 0$, by definition.

$\Leftarrow$ If (B,σ) gives rise to $(N,0)$ then $(N,0)$ gives rise to a split extension of A which is isomorphic to (B,σ). Hence (B,σ) is also split.

$\Leftarrow$(Another way) Since $f_\rho = \delta_2 g$ for some $g \in C^1(A,N)$, let $\rho' = \rho - g$. Then $A^* = \rho'(A)$ is a subalgebra of B complementing N.

Indeed, $\sigma\rho' = \sigma\rho - \sigma g = 1_A$ (because $g(A) \subset N$). Thus, $N \bigoplus \rho'(A) = B$ and

$$\rho'(a_1)\rho'(a_2) = \rho(a_1)\rho(a_2) - \rho(a_1)g(a_2) - g(a_1)\rho(a_2) + 0 =$$

$$f_\rho(a_1,a_2) + \rho(a_1a_2) - a_1.g(a_2) - g(a_1).a_2 = -g(a_1a_2) + \rho(a_1a_2) = \rho'(a_1a_2).\clubsuit$$

Corollary 1. *$H^2(A,-) = (0)$ iff every singular and linearly unital extension of A splits.*

Proposition 3. *The following conditions are equivalent:*

(i) Every unital extension of A with nilpotent kernel splits.

(ii) Every unital singular extension of A splits.

Proof. (ii)$\Leftarrow$(i) We argue by induction on n, the degree of nilpotency of the kernel of the extension.

If $n \leq 2$ then the extension is singular by definition. Assume that $n \geq 2$ and that the result holds for all $k \leq n$. Let (B,σ) be a unital extension of A with nilpotent kernel N, whose degree of nilpotency is $n+1$. Since $N^2 \subset N$, σ factors through B/N^2 via a unique $\widetilde{\sigma}$ with kernel $N/N^2 = \ker\sigma/N^2$ satisfying $(N/N^2)^2 = (0)$.

Thus $(B/N^2, \widetilde{\sigma})$ is a unital singular extension of A, so by Proposition 3.2.1(3) we have $B/N^2 = A^* \bigoplus N/N^2$ for some subalgebra A^* of B/N^2. Write $A^* = C/N^2$ for some subalgebra C of B containing N^2. Since $C/N^2 \simeq A$ there is an epimorphism from C onto A with kernel N^2, and N^2 is nilpotent with degree of nilpotency $\leq n$. By inductive hypothesis, $C = D \bigoplus N^2$ for some subalgebra D of C, and hence of B.

From $B/N^2 = (D \bigoplus N^2/N^2) \bigoplus N/N^2$ we see that $B = D \bigoplus N$. $\clubsuit$

Theorem 1 (Wedderburn-Malcev). *Let R be a commutative ring and A an associative unital R-algebra which is projective as an R-module. Suppose that $H^2(A,-) = (0)$. Then any unital extension (B,σ) of A with nilpotent kernel splits. Moreover if A is separable over R and $B = A_1^* \bigoplus \ker\sigma = A_2^* \bigoplus \ker\sigma$, there is some $n \in \ker\sigma$ such that $A_1^* = (1-n)A_2^*(1-n)^{-1}$.*

Proof. For the existence apply Corollary 1 followed by Proposition 3.2.1(2) to see that every unitary singular extension of A splits. Then use Proposition 3.

For the second part recall that A is separable over R iff $Ext^n_{A^e}(A,-) = (0)$ for all $n \in \mathbb{N}$ iff $H^n(A,-) = (0)$ for all $n \in \mathbb{N}$ (see the previous section and Proposition 2.3.1). Let $\rho_1, \rho_2 \colon A \to B$ be R-algebra maps satisfying $\sigma\rho_1 = \sigma\rho_2 = 1_A$ and $\rho_1(A) = A_1^*$, $\rho_2(A) = A_2^*$. We define a structure of two sided A/R-module on $N = \ker\sigma$ as follows:

$$a.n = \rho_1(a)n \quad n.a = n\rho_2(a)$$

for all $u \in N$ and $a \in A$. All axioms are easily verified. Define $f \colon A \to N$ by $f(a) = \rho_1(a) - \rho_2(a)$. f takes values on N for $\sigma f = 0$. We clearly have $f \in C^1(A,N)$ and direct computation shows that $\delta_2 f = 0$, so that $f \in Z^2(A,N) = B^1(A,N)$, because A is separable over R.

Thus, there is some $n \in N$ such that:

$$\rho_1(a) - \rho_2(a) = f(a) = a.n - n.a = \rho_1(a)n - n\rho_2(a)$$

for all $a \in A$, so that

$$\rho_1(a)(1-n) = (1-n)\rho_2(a)$$

which implies

$$\rho_1(a) = (1-n)\rho_2(a)(1-n)^{-1}$$

since N is nilpotent. The result follows. ♣

We obtain as a corollary:

Theorem 2 (Wedderburn-Malcev, classical version). *Let A be a finite dimensional associative unital algebra over a field $\mathbb{K}$. Suppose that $A/J(A)$ is*

classically separable. Then $A = S_1 \bigoplus J(A)$ *for some subalgebra* S_1 *of* A*, and if* S_2 *also satisfies that, then* $S_1 = (1-n)S_2(1-n)^{-1}$ *for some* $n \in J(A)$*.*

Proof. Let $\sigma\colon A \to A/J(A)$ be the canonical projection. Then the kernel $J(A)$ of the extension (A, σ) of $A/J(A)$ is nilpotent, for A is finite dimensional. Due to Theorem 2.6.1 $A/J(A)$ is separable and hence $H^2(A/J(A), -) = (0)$. Now apply Theorem 1. ♣

3.4. Examples

Example 1. We show that the class of algebras whose 1-cohomology modules are all 0 is strictly contained in the class of algebras whose 2-cohomology modules are all 0. Our example is an adaptation for unital algebras of the original example given in Hochschild [46].

Let R be a commutative ring and A any free module of rank 3 (the rank of A is well-defined and equal to $dim_{R/I} R/I \otimes_R A$ for every maximal ideal I of R). Assume furthermore that R is semisimple and let $(1, a, r)$ be any basis of A over R. There is a unique structure of associative and unital R-algebra on A such that 1 is the multiplicative identity and $aa = a \quad ar = r \quad rr = 0 \quad ra = 0$. We claim that:

(i) A is not separable.

(ii) $H^2(A, -) = (0)$.

Proof. (i) Suppose that A is separable over R. Then A must be semisimple due to Corollary 2.5.2 contradicting the fact that A has a non-zero nilpotent ideal, namely $(r) = Rr$.

(ii) Let M be any two sided A/R module and $f \in Z^2(A, M)$, that is, $f\colon A^2 \to M$ is R-bilinear and for all $a_i \in A$:

$$(*) \qquad 0 = (\delta_3 f)(a_1, a_2, a_3) = a_1 f(a_2, a_3) - f(a_1 a_2, a_3) + f(a_1, a_2 a_3) - f(a_1, a_2) a_3.$$

We must show that there is some R-linear map $g\colon A \to M$ such that $\delta_2 g = f$, that is, for all $a_i \in A$:

$$(**) \qquad f(a_1, a_2) = a_1 g(a_2) - g(a_1 a_2) + g(a_1) a_2.$$

To see this let g be the unique R-linear extension of:

$$g(a) = 2f(a, a)a - f(a, a)$$

$$g(r) = 2f(r, a)a - f(r, a) + f(a, r)a - f(a, r)$$

$$g(1) = f(1, 1)$$

We can restrict the verification of (**) to those pairs (a_1, a_2) where a_1 and a_2 are elements of the basis $(1, a, r)$. We will perform this task in some of the nine possible cases to show how this is done and leave the rest to the reader.

The five cases in which at least one of the a_i is 1 are easy to check. For instance, if $(a_1, a_2) = (1, a)$ then applying (*) to $(1, 1, a)$ we get

$$0 = f(1,a) - f(1,a) + f(1,a) - f(1,1)a = f(1,a) - f(1,1)a$$

while on the other hand

$$\delta_2 g(1,a) = g(a) - g(a) + g(1)a$$

so combining these two equations we get

$$\delta_2 g(1,a) = g(1)a = f(1,1)a = f(1,a).$$

From the other cases the one involving more computational work occurs when $(a_1, a_2) = (a, r)$. In this case:

$$\delta_2 g(a,r) = ag(r) - g(r) + g(a)r = 2af(r,a)a - af(r,a) +$$

$$af(a,r)a - af(a,r) - 2f(r,a)a + f(r,a) - f(a,r)a + f(a,r) + f(a,a)r.$$

Applying (*) to (a, a, r) we see that $f(a,a)r = af(a,r)$. We also apply (*) to (a, r, a) and then multiply the resulting equation on the right and on the left by a to obtain $af(a,r)a = 0$. This gives:

$$\delta_2 g(a,r) = 2af(r,a)a - af(r,a) - 2f(r,a)a + f(r,a) - f(a,r)a + f(a,r).$$

If we now apply (*) again to (a, r, a) and then multiply only on the right by a we get $af(r,a)a = f(r,a)a + f(a,r)a$. Replacing this above yields:

$$\delta_2 g(a,r) = 2f(r,a)a + 2f(a,r)a - af(r,a) - 2f(r,a)a + f(r,a) - f(a,r)a + f(a,r) =$$

$$f(a,r)a - af(r,a) + f(r,a) + f(a,r).$$

But (*) applied to (a,r,a) says that $f(a,r)a - af(r,a) + f(r,a) = 0$ which finally gives $\delta_2 g(a,r) = f(a,r)$, as desired. ♣

Example 2. Let R and A be as in Example 1. Assume furthermore that the $R = \mathbb{K}$ is a field. Under this conditions we can do the following:
(i) Find all the subalgebras of A complementing the radical $J(A)$.
(ii) Given any two of these we find an explicit inner automorphism sending one onto another.

Let $S = \mathbb{K}a \bigoplus \mathbb{K}(1-a)$. We see at once that S is a subalgebra of A and since $(1-a, a, r)$ is also a basis of A it is clear that S complements the ideal $(r) = \mathbb{K}r$ of A. Define the map $\omega\colon A \to \mathbb{K} \times \mathbb{K}$ by

$$A \ni k_0(1-a) + k_1 a + k_2 r \mapsto (k_0, k_1) \in \mathbb{K} \times \mathbb{K}.$$

Since a and $1-a$ are orthogonal idempotents it is immediate to verify that ω is an algebra epimorphism. The kernel of ω is $\mathbb{K}r$. Since $\mathbb{K}r \subset J(A)$ and $\mathbb{K} \times \mathbb{K}$ is semisimple it follows that $\mathbb{K}r = J(A)$. Moreover since $A/J(A) \simeq \mathbb{K} \times \mathbb{K}$ is separable over $\mathbb{K}$ (see Proposition 2.4.4) we know that (ii) is feasible.

Suppose now that S^* is another subalgebra of A satisfying $A = S^* \bigoplus J(A)$. We then have $S^* \simeq A/J(A) \simeq \mathbb{K} \times \mathbb{K}$. It follows from $S^* \simeq \mathbb{K} \times \mathbb{K}$ that $S^* = \mathbb{K}e \bigoplus \mathbb{K}(1-e)$ where $e = k_0(1-a) + k_1 a + k_2 r$ is some non-zero idempotent of A different from 1. From $e = e^2$ we get:

$$k_0(1-a) + k_1 a + k_2 r = k_0^2(1-a) + k_1^2 a + (k_0 + k_1)k_2 r$$

yielding

$$k_0 = k_0^2 \quad k_1 = k_1^2 \quad k_2 = (k_0 + k_1)k_2$$

At this point we use for the first time the fact that the commutative semisimple ring R is an integral domain, that is, that R is the field $\mathbb{K}$. We use this fact to conclude from above that k_0 and k_1 are equal to 0 or 1 but $k_0 \neq k_1$ since $0 \neq e \neq 1$.

We have found all non-zero idempotents e of A. They are of the form $e = a + kr$ and $1 - e$ where k runs through $\mathbb{K}$. It follows that

$$S^* = \mathbb{K}(a + kr) \bigoplus \mathbb{K}(1 - a - kr)$$

for some $k \in \mathbb{K}$. Thus (i) is accomplished.

In order to fulfil (ii) it is evident that it suffices to show how to conjugate S onto S^*. To do so let $n = kr \in J(A)$. Then

$$(1-n)a(1-n)^{-1} = (1-n)a(1+n) = e + kr$$

and

$$(1-n)(1-a)(1-n)^{-1} = (1-n)(1-a)(1+n) = 1 - e - kr$$

We conclude that $S^* = (1-n)S(1-n)^{-1}$.

Example 3. This example shows an algebra A over a field $\mathbb{F}$ such that $A/J(A)$ is semisimple but not separable over $\mathbb{F}$ and no subalgebra of A is isomorphic to $A/J(A)$.

Let $\mathbb{K}$ be any field of characteristic 2 and let $\mathbb{F} = \mathbb{K}(t)$ be the field of rational functions in t with coefficients in $\mathbb{K}$. Let A be any 4 dimensional vector space over $\mathbb{F}$ and $(1, a, b, c)$ a basis of A over $\mathbb{F}$. There is a unique structure of associative and unital $\mathbb{F}$-algebra on A such that 1 is the multiplicative identity and:

$$ab = ba = c \quad b^2 = 0 \quad a^2 = t1 + b$$

Associativity forces the relations:

$$ac = ca = tb \quad bc = cb = c^2 = 0$$

Thus A is commutative. We want to show that:

(i) $A/J(A)$ is semisimple but not separable over $\mathbb{F}$.

(ii) There is no subalgebra of A isomorphic to $A/J(A)$.

Proof.

(i) Let $I = \mathbb{F}b \bigoplus \mathbb{F}c$. We see at once that I is a nilpotent ideal of A and hence $I \subset J(A)$. To see that in fact $I = J(A)$ we define an epimorphism with kernel I from A onto the semisimple $\mathbb{F}$-algebra B, which is now introduced.

Let z be an indeterminate over $\mathbb{F}$ and consider the polynomial $p = z^2 - t \in \mathbb{F}[z]$. Then p is irreducible over $\mathbb{F}$ and we let $B = \mathbb{F}(\sqrt{t})$ be the splitting field of $z^2 - t$

over $\mathbb{F}$. Define $\omega\colon A \to B$ by

$$A \ni k_0 1 + k_1 a + k_2 b + k_3 c \mapsto k_0 1 + k_1 \sqrt{t} \in \mathbb{F}(\sqrt{t})$$

ω is clearly an $\mathbb{F}$-linear epimorphism with kernel I. Moreover is an homomorphism of $\mathbb{F}$-algebras. Indeed,

$$\omega((k_0 1 + k_1 a + k_2 b + k_3 c)(k'_0 1 + k'_1 a + k'_2 b + k'_3 c)) =$$

$$\omega((k_0 k'_0 + k_1 k'_1 t)1 + (k_0 k'_1 + k_1 k'_0)a + (k_1 k'_1 + k_0 k'_2 + k_2 k'_0 +$$

$$k_1 k'_3 t + k_3 k_1 t)b + (k_1 k'_2 k_2 k'_1 + k_0 k'_3 + k_3 k'_0)c) =$$

$$(k_0 k'_0 + k_1 k'_1 t)1 + (k_0 k'_1 + k_1 k'_0)\sqrt{t} =$$

$$\omega(k_0 1 + k_1 a + k_2 b + k_3 c)\omega(k'_0 1 + k'_1 a + k'_2 b + k'_3 c).$$

Since the field B is semisimple it follows $J(A) = I$. Moreover from the fact that B is a non-separable field extension of F we conclude that $A/J(A) = A/I \simeq B$ is semisimple but not separable over $\mathbb{F}$.

(ii) If S is a subalgebra of A isomorphic to $A/J(A) \simeq B$ then there must be some $s \in S$ such that $s^2 = t1$. But $s = k_0 1 + k_1 a + k_2 b + k_3 c$ for some $k_i \in \mathbb{F}$ and $char\mathbb{F} = 2$ yield:

$$t1 = s^2 = k_0^2 1 + k_1^2 a^2 = (k_0^2 + k_1^2)1 + k_1^2 b$$

which implies $k_1 = 0$ and hence $k_0^2 = t$, which is impossible. ♣

Example 4. If a finite dimensional algebra over a field is *commutative* then the classical version of Wedderburn-Malcev Theorem (Theorem 3.3.2) can be obtained using our knowledge of absolute Jordan-Chevalley decompositions (Theorem 1.6.1) as it was done in Proposition 1.8.3. Conversely, we now use Theorem 3.3.2 (whose proof is independent of what we did in Chapter 1) to show the classical version of Theorem 1.6.1. Namely that:

Given a field $\mathbb{K}$, *a finite dimensional vector space* $\mathbf{V}$ *and an endomorphism* x *of* $\mathbf{V}$ *whose minimal polynomial is separable over* $\mathbb{K}$, *there is a unique Jordan-Chevalley decomposition* (s, n) *of* x *such that* $s, n \in \mathbb{K}[x]$.

Proof. Let $A = \mathbb{K}[x]$. If $p_x = p_1^{r_1} \cdots p_k^{r_k}$ is the decomposition of the minimal polynomial of x into distinct monic and irreducible polynomials over $\mathbb{K}$ then $A \simeq \mathbb{K}[t]/p_x$ so that $A/J(A) \simeq (\mathbb{K}[t]/(p_x))/((p_1 \cdots p_k)/(p_x)) \simeq \mathbb{K}[t]/(p_1 \cdots p_k)$. Using the Chinese Reminder Theorem and the separability of the p_i's over $\mathbb{K}$ we see at once that $\mathbb{K}[t]/(p_1 \cdots p_k)$ and hence $A/J(A)$ is a classically separable $\mathbb{K}$-algebra. It follows from Theorem 3.3.2 that $A = S \bigoplus J(A)$ for a unique classically separable subalgebra of A (uniqueness is due to the fact that A is commutative).

Thus $x = s + n$ for unique $s \in S$ and $n \in J(A)$. Observe that:

(i) $[s, n] = 0$.

(ii) n is nilpotent. Indeed, $J(A)$ is nilpotent.

(iii) s is semisimple. This is due to Proposition 1.6.6.

Therefore (s, n) is a Jordan-Chevalley decomposition of x in $\mathbb{K}[x]$.

If (s', n') is another Jordan-Chevalley decomposition of x in $\mathbb{K}[x]$ then:

(iv) $n' \in J(A)$, since $J(A)$ consists of all nilpotent elements of A.

(v) $\mathbb{K}[s'] \cap J(A) = (0)$, again by Proposition 1.6.6.

(vi) $\mathbb{K}[x] = \mathbb{K}[s'] \bigoplus J(A)$, as it is immediate to verify.

From the uniqueness of S it follows that $S = \mathbb{K}[s']$. We conclude right away that $s = s'$ and $n = n'$. ♣

Bibliography

Albert, A. A.

[61] Structure of Algebras, Amer. Math. Soc. Colloq. Publ. Vol XXIV.

Atiyah, M. F. and Macdonald, I. G.

[69] Introduction to Commutative Algebra. Addison-Wesley Publishing Company, Inc., Reading, Mass.

Auslander, M. and Goldman, O.

[60] The Brauer group of a commutative ring. Trans. Amer. Math. Soc. 97, 367-409.

Bass, H.

[67] Lectures on Topics in Algebraic K-Theory, Bombay.

Bourbaki, N.

[90] Elements of Mathematics. Algebra II. Chapters 4-7. Springer-Verlag, Berlin.

Caserta, F.

[91] Eigenvalues in infinite Dimensions. Linear and Multilinear Algebra 28, 195-201.

Chevalley, C.

[51] Theorie des Groupes de Lie. Hermann, Paris.

DeMeyer, F. and Ingraham, E.

[71] Separable Algebras over Commutative Rings. Lecture Notes in Mathematics 181. Springer-Verlag, Berlin.

Fuchs, L.

[70] Infinite abelian groups, Volume I. Academic Press, New York and London.

Hochschild, G.

[45] On the cohomology groups of an associative algebra. Ann. Math.(2) 46, 56-87.

[46] On The cohomology theory for associative algebras. Ann. Math.(2) 47, 568-579.

Hoffman K. and Kunze R.

[61] Linear Algebra. Prentice-Hall, Englewood Cliffs, N. J.

Hungerford, T. W.

[74] Algebra. Graduate Texts in Mathematics 73. Springer-Verlag, Berlin.

Ingraham,E. C.

[66] Inertial subalgebras of algebras over a commutative ring. Trans. Amer. Math. Soc. 124, 77-93.

Jacobson, N.

[74] Basic Algebra I. W. H. Freeman and Company, San Francisco.

[80] Basic Algebra II. W. H. Freeman and Company, San Francisco.

Knight, J. T.

[71] Commutative Algebra. London Mathematical Society. Lecture Note Series 5. Cambridge University Press.

Micali, A.

[83] Estructuras algebraicas VII (Estructuras de algebras). Secretaria General de la Organizacion de los Estados Americanos. Programa regional de Desarrollo Cientifico y Tecnologico, Washington, D.C.

Moody, R. V. and Pianzola, A.

[To appear] Lie algebras with triangular decompositions. John Wiley & Sons, Inc, New York.

Pierce, R. S.

[82] Associative Algebras. Graduate Texts in Mathematics 88. Springer-Verlag, Berlin.

Rotman, J. J.

[79] An introduction to homological algebra. Academic Press, Inc. New York and London.

Rowen, L.

[88] Ring Theory, Volume I. Academic Press, Inc. New York and London.

[88] Ring Theory, Volume II. Academic Press, Inc. New York and London.

Stewart, I.

[89] Galois Theory, Second edition. Chapman and Hall, London, New York.